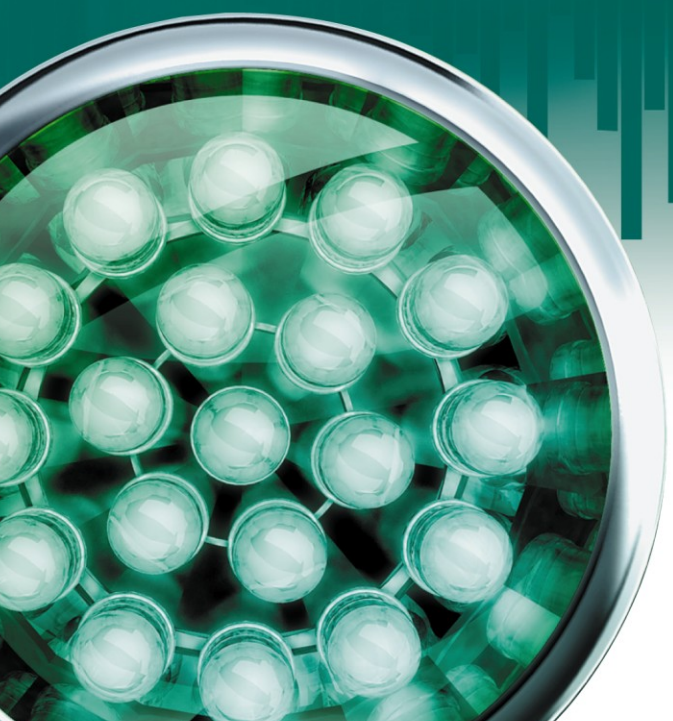
Kaspersky Anti-Virus 2010

MANUAL DE UTILIZADOR

VERSÃO DO PROGRAMA: 9.0 CORRECÇÃO CRÍTICA 2



KASPERSKY lab

Caro Utilizador!

Obrigado por escolher o nosso produto. Esperamos que esta documentação o ajude no seu trabalho e lhe forneça respostas à maioria das questões relativas a este produto de software.

Qualquer tipo de reprodução ou distribuição de quaisquer materiais, incluindo na forma traduzida, só é permitida com a autorização escrita da Kaspersky Lab.

Este documento e as imagens gráficas relacionadas com o mesmo podem ser utilizados, exclusivamente, para fins informativos, não-comerciais e pessoais.

Este documento pode ser alterado sem notificação adicional. Pode encontrar a versão mais recente deste documento no site da Kaspersky Lab: http://www.kaspersky.com/docs.

A Kaspersky Lab não assume qualquer responsabilidade pelo conteúdo, qualidade, relevância ou exactidão de quaisquer materiais utilizados neste documento, cujos direitos sejam detidos por terceiros, ou pelos potenciais danos associados à utilização de tais documentos.

Este documento inclui marcas comerciais registadas e marcas de serviços que são propriedade dos respectivos detentores.

Data de revisão: 10/8/09

© 1997-2009 Kaspersky Lab ZAO. Todos os direitos reservados.

http://www.kaspersky.pt
http://support.kaspersky.pt

ÍNDICE

INTRODUÇÃO 9
Kit de distribuição 9
Serviços fornecidos a utilizadores registados 10
Requisitos de hardware e software de sistema 10
KASPERSKY ANTI-VIRUS 2010 11
Obter informação sobre a aplicação 11
Fontes de informação para pesquisar por si próprio 11
Contactar o Departamento de Vendas 12
Contactar o Serviço de Suporte Técnico 12
Discutir as aplicações da Kaspersky Lab no Fórum da Internet 13
O QUE HÁ DE NOVO NO KASPERSKY ANTI-VIRUS 2010 14
O CONCEITO DA PROTECÇÃO DO SEU COMPUTADOR 15
Componentes de protecção 15
Tarefas de verificação de vírus 17
Actualização 17
Protecção dos dados e das actividades on-line 17
Assistentes e Ferramentas 18
Funcionalidades de suporte do programa 18
INSTALAR O KASPERSKY ANTI-VIRUS 20
Passo 1. Procurar uma versão mais recente da aplicação 21
Passo 2. Verificar se o sistema satisfaz os requisitos de instalação 21
Passo 3. Seleccionar o tipo de instalação 21
Passo 4. Visualizar o Contrato de Licença 22
Passo 5. Declaração de Recolha de Dados do Kaspersky Security Network 22
Passo 6. Seleccionar a pasta de instalação 22
Passo 7. Seleccionar as componentes da aplicação a instalar 22
Passo 8. Utilizar configurações da aplicação guardadas numa instalação anterior 23
Passo 9. Procurar outras aplicações antivírus 23
Passo 10. Preparação final para a instalação 24
Passo 11. Concluir a instalação 24
COMO COMEÇAR 25
Assistente de Configuração da Aplicação 26
Passo 1. Activar a aplicação 26
Passo 2. Seleccionar um modo de protecção 28
Passo 3. Configurar as actualizações da aplicação 28
Passo 4. Restringir o acesso à aplicação 29
Passo 5. Seleccionar ameaças detectáveis 29
Passo 6. Fechar o Assistente 29
Actualizar a aplicação 29
Verificação de vírus no computador 30
Verificação de vulnerabilidades no computador 30
Gerir a licença 31
Subscrição para a renovação automática da licença 31
Participar no Kaspersky Security Network 32

Gestão de Segurança ... 33
Estado de protecção ... 35
Pausar a protecção ... 35
INTERFACE DA APLICAÇÃO ... 37
Ícone da área de notificação ... 37
Menu de contexto ... 38
Janela principal do Kaspersky Anti-Virus ... 39
Notificações ... 41
Janela de configuração da aplicação ... 41
PROTECÇÃO DO SISTEMA DE FICHEIROS DO COMPUTADOR ... 42
Algoritmo de funcionamento da componente ... 43
Alterar o nível de segurança dos ficheiros e da memória ... 44
AError! Bookmark not defined.lterar as acções a executar com objectos detectados ... 45
Criar um âmbito de protecção ... 45
Utilizar a análise heurística ... 46
Optimização da verificação ... 47
Verificação de ficheiros compostos ... 47
Verificar ficheiros compostos extensos ... 48
Alterar o modo de verificação ... 48
Tecnologia de verificação ... 49
Pausar a componente: criar um agendamento ... 49
Pausar a componente: criar uma lista de aplicações ... 50
Restaurar as predefinições de protecção ... 51
PROTECÇÃO DE E-MAILS ... 52
Algoritmo de funcionamento da componente ... 53
Alterar o nível de segurança da protecção de e-mail ... 54
Alterar as acções a executar com objectos detectados ... 54
Criar um âmbito de protecção ... 55
Verificar e-mails no Microsoft Office Outlook ... 56
Verificação de e-mails no The Bat! ... 56
Utilizar a análise heurística ... 57
Verificação de ficheiros compostos ... 57
Filtrar anexos ... 58
Restaurar as predefinições da protecção de e-mail ... 58
PROTECÇÃO DO TRÁFEGO DE INTERNET ... 59
Algoritmo de funcionamento da componente ... 60
Alterar o nível de segurança do tráfego de HTTP ... 61
Alterar as acções a executar com objectos detectados ... 61
CError! Bookmark not defined.riar um âmbito de protecção ... 62
Seleccionar o tipo de verificação ... 62
Conselheiro de URLs da Kaspersky ... 63
Utilizar a análise heurística ... 64
Optimização da verificação ... 64
Restaurar as predefinições de protecção da Internet ... 65
PROTEGER O TRÁFEGO DE PROGRAMAS DE MENSAGENS INSTANTÂNEAS ... 66
AError! Bookmark not defined.lgoritmo de funcionamento da componente ... 67
Criar um âmbito de protecção ... 67

Seleccionar o método de verificação ... 68
Utilizar a análise heurística ... 68
DEFESA PROACTIVA ... 69
Utilizar a lista de actividades perigosas ... 69
Alterar a regra de monitorização de actividades perigosas ... 70
Criar um grupo de aplicações confiáveis ... 71
Controlo das contas do sistema ... 71
VERIFICAÇÃO DO COMPUTADOR ... 72
Verificação de vírus ... 72
Iniciar a tarefa de verificação de vírus ... 74
Criar um atalho para a execução de tarefas ... 75
Criar uma lista de objectos a verificar ... 75
Alterar o nível de segurança do tráfego de HTTP ... 76
Alterar as acções a executar com objectos detectados ... 76
Alterar o tipo de objectos a verificar ... 77
Optimização da verificação ... 78
Verificar discos removíveis ... 78
Verificação de ficheiros compostos ... 79
Tecnologia de verificação ... 80
Alterar o método de verificação ... 80
Modo de execução criar um agendamento ... 81
Modo de execução especificar uma conta de utilizador ... 82
Características da inicialização de tarefas agendadas ... 82
Restaurar as predefinições de verificação ... 82
Verificação de vulnerabilidades ... 83
Iniciar a tarefa de verificação de vulnerabilidades ... 84
Criar um atalho para a execução de tarefas ... 84
Criar uma lista de objectos a verificar ... 84
Modo de execução criar um agendamento ... 85
Modo de execução especificar uma conta de utilizador ... 86
ACTUALIZAÇÃO ... 87
Iniciar a Actualização ... 88
Reverter a última actualização ... 89
Seleccionar uma origem de actualização ... 89
Usar um servidor de proxy ... 90
Configurações regionais ... 90
Acções após a actualização ... 90
Actualizar a partir de uma pasta local ... 91
Alterar o modo de execução da tarefa de actualização ... 92
Executar actualizações com outra conta de utilizador ... 92
CONFIGURAÇÃO DAS DEFINIÇÕES DA APLICAÇÃO ... 93
Protecção ... 94
Activar / desactivar a protecção do computador ... 95
Iniciar o Kaspersky Anti-Virus com a inicialização do sistema operativo ... 95
Utilizar o modo de protecção interactiva ... 96
Restringir o acesso ao Kaspersky Anti-Virus ... 96
Antivírus de Ficheiros ... 97

Antivírus de E-mail ... 97
Antivírus de Internet ... 98
Antivírus de MI ... 99
Defesa Proactiva ... 99
Verificação ... 100
Actualização ... 101
Configuração ... 101
Autodefesa do Kaspersky Anti-Virus ... 101
Tecnologia de desinfecção avançada ... 102
Utilizar o Kaspersky Anti-Virus num Computador Portátil ... 102
Desempenho do computador durante a execução de tarefas ... 103
Exportar / importar as definições do Kaspersky Anti-Virus ... 103
Restaurar as predefinições ... 104
Ameaças e exclusões ... 104
Rede ... 108
Notificações ... 112
Relatórios e Armazenamento ... 113
Informação de retorno ... 116
Aparência da aplicação ... 117
Utilizar os perfis do Kaspersky Anti-Virus ... 118
FUNCIONALIDADES ADICIONAIS ... 119
Teclado virtual ... 119
Disco de Recuperação ... 120
Criar o disco de recuperação ... 121
Iniciar o computador com o disco de recuperação ... 121
Configuração do navegador ... 122
Restaurar o sistema após uma infecção ... 123
Assistente de Limpeza de vestígio de actividade ... 124
RELATÓRIOS ... 125
Seleccionar uma componente ou tarefa para criar um relatório ... 126
Gerir o agrupamento de informação no relatório ... 126
Notificação sobre a criação de relatórios ... 127
Seleccionar o tipo de eventos ... 127
Exibir Dados no Ecrã ... 128
Exibir estatísticas avançadas ... 129
Guardar o relatório num ficheiro ... 129
Utilizar a filtragem complexa ... 130
Procura de eventos ... 131
NOTIFICAÇÕES ... 132
Objecto malicioso detectado ... 133
Objecto não pode ser desinfectado ... 134
Necessidade de tratamento especial ... 134
Objecto perigoso detectado no tráfego ... 134
Objecto suspeito detectado ... 135
Actividade perigosa detectada no sistema ... 136
Processo oculto detectado ... 136
Detecção de tentativa de acesso ao registo do sistema ... 137
Ataque de phishing detectado ... 137

Link suspeito detectado ... 138
Certificado inválido detectado ... 138
VALIDAR A CONFIGURAÇÃO DO KASPERSKY ANTI-VIRUS ... 139
Testar o "vírus" EICAR e suas variantes ... 139
Testar a protecção do tráfego de HTTP ... 140
Testar a protecção do tráfego de SMTP ... 141
Validar a configuração do Antivírus de Ficheiros ... 141
Validar a configuração das tarefas de verificação de vírus ... 141
TRABALHAR COM A APLICAÇÃO A PARTIR DA LINHA DE COMANDOS ... 142
Gerir componentes e tarefas da aplicação ... 143
Verificação de vírus ... 145
Actualizar a aplicação ... 148
Reverter a última actualização ... 149
Exportar as definições de protecção ... 149
Importar as definições de protecção ... 150
Iniciar a aplicação ... 150
Parar a aplicação ... 150
Criar um ficheiro de rastreio ... 150
Visualizar a Ajuda ... 151
Códigos de retorno da interface da linha de comandos ... 151
ELIMINAR PROBLEMAS ... 152
Criar um relatório sobre o estado do sistema ... 152
Criar um ficheiro de rastreio ... 153
Enviar ficheiros de dados ... 154
Executar script AVZ ... 155
DECLARAÇÃO DE RECOLHA DE DADOS DO KASPERSKY SECURITY NETWORK ... 156
UTILIZAR CÓDIGO DE TERCEIROS ... 160
Biblioteca Crypto C (biblioteca de software de segurança de dados) ... 161
Biblioteca Fastscript 1.9 ... 161
Biblioteca Libnkfm 7.4.7.7 ... 161
Biblioteca GNU bison parser ... 162
Biblioteca AGG 2.4 ... 162
Biblioteca OpenSSL 0.9.8d ... 163
Biblioteca Gecko SDK 1.8 ... 164
Biblioteca Zlib 1.2 ... 164
Biblioteca Libpng 1.2.8, 1.2.29 ... 164
Biblioteca Libnkfm 2.0.5 ... 164
Biblioteca Expat 1.2, 2.0.1 ... 165
Biblioteca Info-ZIP 5.51 ... 165
Biblioteca Windows Installer XML (WiX) 2.0 ... 166
Biblioteca Passthru ... 168
Biblioteca Filter ... 168
Biblioteca Netcfg ... 169
Biblioteca Pcre 3.0 ... 169
Biblioteca RFC1321-based (RSA-free) MD5 ... 169
Biblioteca Windows Template Library (WTL 7.5) ... 169
Biblioteca Libjpeg 6b ... 172

Biblioteca Libungif 3.0 ... 173
Biblioteca Libxdr ... 173
Biblioteca Tiniconv - 1.0.0 ... 174
Biblioteca Bzip2/libbzip2 1.0.5 ... 179
Biblioteca Libspf2-1.2.9 ... 179
Biblioteca Protocol Buffer ... 180
GLOSSÁRIO ... 181
KASPERSKY LAB ... 189
CONTRATO DE LICENÇA ... 190
ÍNDICE ... 196

INTRODUÇÃO

NESTA SECÇÃO:

Kit de distribuição 9

Serviços fornecidos a utilizadores registados 10

Requisitos de hardware e software de sistema 10

KIT DE DISTRIBUIÇÃO

Pode adquirir o Kaspersky Anti-Virus numa caixa, através dos nossos parceiros, ou adquiri-la online através das lojas da Internet, tais como a secção **Loja Online** do site http://www.kaspersky.pt.

Se comprar a versão do programa em caixa, esta incluirá:

- Um envelope selado com um CD de instalação contendo os ficheiros do programa e documentação em formato PDF.
- Documentação impressa, nomeadamente os documentos Manual de Utilizador e Guia Rápido de Instalação.
- O Contrato de Licença (dependendo da região).
- O cartão de activação, que contém um código de activação e o manual de activação da aplicação (dependendo da região).

O Contrato de Licença do Utilizador Final é um acordo legal entre você e a Kaspersky Lab, que especifica os termos pelos quais poderá usar o software que adquiriu.

Leia o CLUF cuidadosamente!

Se não concordar com os termos do CLUF, poderá devolver o produto embalado ao parceiro onde o comprou e ser reembolsado pela quantidade que pagou pelo programa, desde que o envelope com o disco de instalação ainda esteja selado.

Ao abrir o disco selado de instalação, aceitará todos os termos do CLUF.

Antes de romper o selo do envelope do disco de instalação, leia cuidadosamente o CLUF.

Se comprar o Kaspersky Anti-Virus na Loja Online, irá transferir o produto a partir do site da Kaspersky Lab. O presente Manual de Utilizador está incluído no pacote de instalação. Ser-lhe-á enviado um código de activação por e-mail, depois de ter efectuado o pagamento.

SERVIÇOS FORNECIDOS A UTILIZADORES REGISTADOS

A Kaspersky Lab oferece a todos os utilizadores legalmente registados um pacote de serviços abrangente, permitindo-lhes melhorar o desempenho da aplicação.

Depois de adquirir uma licença, você torna-se num utilizador registado e, durante o período da sua licença, ser-lhe-ão fornecidos os seguintes serviços:

- actualizações horárias das bases de dados da aplicação e actualizações do pacote do software;
- suporte em questões relacionadas com a instalação, configuração e utilização do produto de software adquirido. Os serviços serão prestados por telefone ou e-mail;
- notificações sobre a publicação de novos produtos da Kaspersky Lab e sobre novos vírus que apareçam a nível mundial. Este serviço está disponível para os utilizadores que subscreveram a newsletter da Kaspersky Lab no site do Serviço de Suporte Técnico (http://support.kaspersky.com/subscribe).

Não é fornecido suporte em questões relacionadas com o desempenho e utilização dos sistemas operativos ou outras tecnologias que não pertençam à Kaspersky Lab.

REQUISITOS DE HARDWARE E SOFTWARE DE SISTEMA

Para o funcionamento adequado do Kaspersky Anti-Virus 2010, o computador deve obedecer aos seguintes requisitos mínimos:

Requisitos gerais:

- 375 MB de espaço livre em disco.
- CD-ROM (para a instalação do Kaspersky Anti-Virus 2010 a partir do CD de instalação).
- Microsoft Internet Explorer 6.0 ou superior (para a actualização das bases da aplicação e dos módulos do software através da Internet).
- Microsoft Windows Installer 2.0.

➡ *Microsoft Windows XP Home Edition (Service Pack 2),* Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition*:*

- Processador Intel Pentium 300 MHz ou superior (ou compatível)
- 256 MB de RAM livre.

➡ *Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:*

- Processador Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) ou superior (ou compatível).
- 512 MB de RAM livre.

➡ *Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:*

- Processador Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) ou superior (ou compatível).
- 1 GB de RAM livre (32-bit); 2 GB de RAM livre (64-bit).

KASPERSKY ANTI-VIRUS 2010

O Kaspersky Anti-Virus 2010 é uma nova geração de soluções de segurança de informação.

O que distingue, verdadeiramente, o Kaspersky Anti-Virus 2010 dos outros softwares, inclusive dos outros produtos da Kaspersky Lab, é a abordagem multi-facetada no que respeita à segurança de dados no computador do utilizador.

NESTA SECÇÃO:

Obter informação sobre a aplicação 11

OBTER INFORMAÇÃO SOBRE A APLICAÇÃO

Se tem alguma questão relativamente à aquisição, instalação ou utilização da aplicação, as respostas estão facilmente disponíveis.

A Kaspersky Lab fornece diversas fontes de informação sobre a aplicação. Pode escolher as mais adequadas, dependendo da urgência e importância das suas questões.

NESTA SECÇÃO:

Fontes de informação para pesquisar por si próprio 11

Contactar o Departamento de Vendas 12

Contactar o Serviço de Suporte Técnico 12

Discutir as aplicações da Kaspersky Lab no Fórum da Internet 13

FONTES DE INFORMAÇÃO PARA PESQUISAR POR SI PRÓPRIO

Pode consultar as seguintes fontes de informação sobre a aplicação:

- página da aplicação no site da Kaspersky Lab;
- página da aplicação no site do Serviço de Suporte Técnico (na Base de Conhecimento);
- página do serviço de Suporte do FastTrack;
- Sistema de Ajuda;
- documentação.

Página da aplicação no site da Kaspersky Lab

http://www.kaspersky.com/kaspersky_anti-virus

Esta página irá fornecer-lhe informação geral sobre a aplicação e as respectivas funcionalidades e opções.

Página da aplicação no site do Serviço de Suporte Técnico (na Base de Conhecimento)

http://support.kaspersky.com/kav2010

Nesta página irá encontrar os artigos criados pelos especialistas do Serviço de Suporte Técnico.

Estes artigos contêm informações úteis, recomendações e perguntas frequentes sobre a aquisição, instalação e utilização da aplicação. Estas estão organizadas segundo o assunto, tais como Gerir ficheiros de chave, Configurar actualizações da base de dados ou Eliminar falhas de funcionamento. Os artigos podem fornecer respostas às questões referentes não só a esta aplicação, mas também aos outros produtos da Kaspersky Lab. Estes também podem conter notícias do Serviço de Suporte Técnico.

Serviço de Suporte do FastTrack

Nesta página do serviço, pode encontrar a base de perguntas frequentes com respostas, a qual é regularmente actualizada. Para utilizar este serviço, vai precisar de uma ligação à Internet.

Para aceder à página do serviço, na janela principal da aplicação clique na ligação **Suporte** e, na janela que se abre, clique no botão **Suporte do FastTrack**.

Sistema de Ajuda

O pacote de instalação da aplicação inclui o ficheiro completo do contexto da ajuda, que contém informação sobre como gerir a protecção do computador (ver o estado de protecção, verificar a existência de vírus em várias áreas do computador, executar outras tarefas), bem como a informação sobre cada janela da aplicação, como por exemplo a lista das suas configurações adequadas e sua descrição e a lista de tarefas a executar.

Para abrir o ficheiro de ajuda, clique no botão **Ajuda** na janela desejada ou prima a tecla **<F1>**.

Documentação

O pacote de instalação do Kaspersky Anti-Virus inclui o documento **Manual de Utilizador** (em formato PDF). Este documento contém descrições das funcionalidades e opções da aplicação, assim como dos principais algoritmos de funcionamento.

CONTACTAR O DEPARTAMENTO DE VENDAS

Pode enviar as suas questões para os especialistas do Departamento de Vendas, através do endereço de e-mail: retail@kaspersky.pt.

CONTACTAR O SERVIÇO DE SUPORTE TÉCNICO

Se já comprou o Kaspersky Anti-Virus, pode obter informação sobre o mesmo a partir do serviço de Suporte Técnico por telefone ou pela Internet.

Os especialistas do serviço de Suporte Técnico irão responder a todas as suas questões sobre a instalação e utilização da aplicação. Caso o seu computador tenha sido infectado, eles também o ajudarão a eliminar as consequências das actividades do software malicioso.

Antes de contactar o Serviço de Suporte Técnico, por favor leia as Regras do suporte para os produtos da Kaspersky Lab (http://support.kaspersky.com/support/rules).

Suporte Técnico por e-mail

Pode colocar as suas questões em Russo, Inglês, Alemão, Francês ou Espanhol.

O Serviço de Suporte Técnico irá responder ao seu pedido na sua Conta Kaspersky (https://my.kaspersky.com) e através do endereço de e-mail que especificou no seu pedido.

No formulário on-line do pedido, descreva o problema que encontrou o mais detalhadamente possível. Especifique as seguintes informações nos campos obrigatórios:

- **Tipo de pedido**. Seleccione o assunto que melhor corresponde ao problema. Por exemplo: Problema de instalação/desinstalação do produto ou Problema na procura/eliminação de vírus. Se não encontrar nenhum tópico adequado, seleccione o tópico "Questão Geral".
- **Nome e número da versão da aplicação**.
- **Texto do pedido**. Descreva o problema que encontrou o mais detalhadamente possível.
- **ID de cliente e password**. Insira o número de cliente e a password que recebeu durante o registo no site do serviço de Suporte Técnico.
- **Endereço de e-mail**. O serviço de Suporte Técnico irá enviar a resposta à sua questão para este endereço de e-mail.

Suporte Técnico por telefone

Se tem questões relativamente à selecção ou aquisição do Kaspersky Internet Security ou sobre como prolongar a sua licença, por favor contacte con

IportalMais**:**

Tel.: +351 22 510 64 76

Minitel :

Tel.: +351 21 381 09 22

DISCUTIR AS APLICAÇÕES DA KASPERSKY LAB NO FÓRUM DA INTERNET

Se a sua questão não requer uma resposta urgente, pode discuti-la com os especialistas da Kaspersky Lab e outros utilizadores no nosso fórum na Internet, através do endereço http://forum.kaspersky.com.

Neste fórum pode visualizar os tópicos existentes, deixar os seus comentários, criar novos tópicos e utilizar o motor de pesquisa.

O QUE HÁ DE NOVO NO KASPERSKY ANTI-VIRUS 2010

O Kaspersky Anti-Virus 2010 é uma ferramenta abrangente de protecção de dados. A protecção multi-facetada abrange todos os canais de transferência e intercâmbio de dados. A configuração flexível fornecida para cada uma das componentes permite aos utilizadores adaptar o Kaspersky Anti-Virus às suas necessidades específicas.

Vamos analisar em maior detalhe as inovações do Kaspersky Anti-Virus 2010.

Novidades na protecção:

- A nova componente Antivírus de MI (ver página 66) garante o funcionamento seguro de diversas aplicações de mensagens instantâneas. A componente verifica as mensagens quanto à presença de objectos maliciosos.

- O Kaspersky Anti-Virus inclui o Conselheiro de URLs da Kaspersky (ver página 63) gerido pelo Antivírus de Internet. Este módulo verifica se os links existentes na página de Internet pertencem à lista de endereços de Internet suspeitos e de phishing. Este módulo é integrado nos navegadores Microsoft Internet Explorer e Mozilla Firefox como uma extensão (plug-in).

- A monitorização do acesso a sites de phishing e a protecção contra ataques de phishing são executadas verificando os links existentes em mensagens e páginas de Internet e utilizando a base de dados de endereços phishing quando for detectada uma tentativa de acesso a sites. Você pode verificar os endereços de Internet se estiverem incluídos na lista de endereços de phishing. Esta opção só está disponível para o Antivírus de Internet (ver página 62) e o Antivírus de MI (ver página 68).

- Uma nova ferramenta, chamada Verificação de vulnerabilidades (ver página 83), foi adicionada à lista de tarefas de verificação. Esta facilita a detecção e eliminação de ameaças de segurança e vulnerabilidades nas aplicações instaladas no seu computador e nas configurações do sistema operativo.

Novidades na interface:

- Foi implementada uma nova abordagem da gestão da protecção, denominada de Protecção. A protecção do computador é garantida em três dimensões diferentes: ficheiros e dados pessoais do utilizador, objectos do sistema operativo e aplicações instaladas no computador, bem como as actividades de rede. A cada uma das dimensões de protecção é aplicado um conjunto específico de componentes do Kaspersky Anti-Virus. Através da secção Protecção, o utilizador pode saber qual a componente que fornece protecção a uma determinada categoria de recursos e aceder, rapidamente, à edição das respectivas configurações.

- Os Assistentes e Ferramentas (ver página 18), que ajudam a executar tarefas específicas para fornecer a segurança do computador, estão agrupadas na secção **Segurança+**.

O CONCEITO DA PROTECÇÃO DO SEU COMPUTADOR

O Kaspersky Anti-Virus garante a protecção do seu computador contra ameaças conhecidas e novas. Cada tipo de ameaça é processado por uma determinada componente da aplicação. Isto torna a configuração flexível com opções de fácil configuração para todas as componentes, as quais podem ser adaptadas às necessidades de um utilizador em específico ou da empresa como um todo.

O Kaspersky Anti-Virus inclui as seguintes ferramentas de protecção:

- Componentes de protecção (ver página 15), que fornecem a protecção de:
  - ficheiros e dados pessoais;
  - sistema;
  - actividades de rede.
- Tarefas de verificação de vírus (ver página 17) utilizadas para verificar a existência de vírus em ficheiros individuais, pastas, discos, áreas especificadas ou o computador como um todo.
- Actualização (ver página17), garantindo o estado actualizado dos módulos internos da aplicação e das bases de dados utilizadas para verificar programas maliciosos.
- Assistentes e Ferramentas (ver página 18) que facilitam a execução de tarefas durante o funcionamento do Kaspersky Anti-Virus.
- Funcionalidades de suporte (ver página 18) que fornecem informação de suporte para trabalhar com o programa e expandir as capacidades do mesmo.

NESTA SECÇÃO:

Componentes de protecção 15

Tarefas de verificação de vírus 17

Actualização 17

Protecção dos dados e das actividades on-line 17

Assistentes e Ferramentas 18

Funcionalidades de suporte do programa 18

COMPONENTES DE PROTECÇÃO

As seguintes componentes de protecção permitem a defesa do seu computador em tempo real:

Antivírus de Ficheiros (ver página 42)

O Antivírus de Ficheiros monitoriza o sistema de ficheiros do computador. Verifica todos os ficheiros que possam ser abertos, executados ou guardados no seu computador e todas as unidades de disco ligadas. O Kaspersky Anti-Virus intercepta todas as tentativas para aceder a um ficheiro e verifica o ficheiro quanto à existência de vírus conhecidos. O ficheiro apenas pode ser alvo de processamento adicional, caso não esteja infectado ou se for desinfectado com sucesso pela aplicação. Se, por qualquer razão, um ficheiro não puder ser desinfectado, este será apagado, sendo guardada uma cópia do ficheiro na Cópia de Segurança ou sendo movido para a Quarentena.

Antivírus de E-mail (ver página 52)

O Antivírus de E-mail verifica todos os e-mails recebidos e enviados no seu computador. Analisa os e-mails quando à presença de programas maliciosos. O e-mail apenas é disponibilizado ao destinatário se não contiver objectos perigosos. A componente também analisa os e-mails para detectar phishing.

Antivírus de Internet (ver página 59)

O Antivírus de Internet intercepta e bloqueia scripts em sites, caso representem uma ameaça. Todo o tráfego HTTP é sujeito a uma inspecção rigorosa. A componente também analisa as páginas de Internet para detectar phishing.

Antivírus de MI (ver página 66)

O Antivírus de MI garante a utilização segura das comunicações na Internet. Esta componente protege a informação que entra no seu computador através dos protocolos de MI. O Antivírus de MI garante o funcionamento seguro de diversas aplicações de mensagens instantâneas.

Defesa Proactiva (ver página 69)

A Defesa Proactiva permite detectar um novo programa malicioso antes de este executar a sua actividade maliciosa. A componente foi concebida em torno da monitorização e análise do comportamento de todas as aplicações instaladas no seu computador. Com base nas acções executadas por uma aplicação, o Kaspersky Anti-Virus toma uma decisão. A aplicação é potencialmente perigosa. Por isso, o seu computador está protegido não só em relação a vírus conhecidos, mas também relativamente a novos vírus que ainda não foram descobertos.

Anti-Phishing

A componente, integrada no Antivírus de Internet e no Antivírus de MI, permite verificar endereços de Internet para ver se estão incluídos na lista de endereços de phishing e suspeitos.

Algumas componentes de protecção apenas estão disponíveis no Kaspersky Internet Security 2010. Entre as quais:

Controlo das Aplicações

O Controlo das Aplicações regista as acções executadas pelas aplicações no sistema e gere as actividades das aplicações, de acordo com o grupo no qual a componente as classifica. Para cada grupo de aplicações é definido um conjunto de regras. Estas regras gerem o acesso das aplicações a diversos recursos.

Firewall

A Firewall garante a segurança do seu trabalho em redes locais e na Internet. A componente filtra todas as actividades de rede, através de dois tipos de regras: *regras para aplicações* e *regras de pacotes*.

Bloqueio de Ataques de Rede

O Bloqueio de Ataques de Rede é carregado quando o sistema operativo se inicia e verifica o tráfego de rede de entrada quanto à existência de actividades características de ataques de rede. Se forem detectadas tentativas de ataque ao computador, o Kaspersky Anti-Virus bloqueia todas as actividades de rede do computador atacante direccionadas ao seu computador.

Anti-Spam

O Anti-Spam está integrado no cliente de e-mail instalado no seu computador e monitoriza todos os e-mails recebidos quanto à presença de spam. Todos os e-mails que contenham spam são marcados com um cabeçalho especial. Também é fornecida a opção de configurar o Anti-Spam para o processamento de spam (apagar automaticamente, mover para uma pasta especial, etc.) A componente também analisa os e-mails para detectar phishing.

Monitor de Rede

A componente foi concebida para ver informação sobre a actividade de rede em tempo real.

Anti-Banner

O Anti-Banner bloqueia as informações publicitárias localizadas em faixas especiais (banners) exibidas on-line ou integradas na interface de programas instalados no seu computador.

Controlo Parental

A componente Controlo Parental monitoriza o acesso dos utilizadores aos recursos da Internet. O principal objectivo do Controlo Parental é restringir o acesso a sites adultos que lidem com pornografia, armas, abuso de drogas, crueldade, violência, etc., assim como a sites que poderiam levar ao desperdício de tempo (salas de conversação, sites de jogos) ou de dinheiro (lojas on-line, leilões).

TAREFAS DE VERIFICAÇÃO DE VÍRUS

Para além da protecção constante de todas as vias através das quais os programas maliciosos podem penetrar, é extremamente importante verificar, periodicamente, a existência de vírus no seu computador. Isto é necessário para eliminar a possibilidade de propagação de programas maliciosos que ainda não foram descobertos pelas componentes de segurança, por exemplo, porque o nível de segurança é baixo ou por outras razões.

O Kaspersky Anti-Virus inclui as seguintes tarefas de verificação de vírus:

- **Verificação de Objectos**. Verifica objectos seleccionados pelo utilizador. Pode verificar qualquer objecto no sistema de ficheiros do computador.

- **Verificação Completa**. Uma verificação minuciosa de todo o sistema. Por defeito, são verificados os seguintes objectos: memória do sistema, programas carregados ao iniciar, cópia de segurança do sistema, bases de dados de e-mail, discos rígidos, meios de armazenamento removíveis e unidades de rede.

- **Verificação Rápida**. Verificação de vírus dos objectos de inicialização do sistema operativo.

ACTUALIZAÇÃO

Para bloquear qualquer ataque de rede, apagar um vírus ou outro programa malicioso, o Kaspersky Anti-Virus deve ser regularmente actualizado. A componente **Actualizações** foi concebida para esse fim. Esta gere a actualização das bases de dados da aplicação e dos módulos utilizados pela aplicação.

O serviço de distribuição de actualizações permite guardar numa pasta local as actualizações das bases de dados e dos módulos do programa transferidas a partir dos servidores da Kaspersky Lab e depois torná-las acessíveis a outros computadores da rede para reduzir o tráfego de Internet.

PROTECÇÃO DOS DADOS E DAS ACTIVIDADES ON-LINE

O Kaspersky Anti-Virus protege os dados do seu computador contra os programas maliciosos e o acesso não autorizado, assim como garante a segurança das suas operações na rede local e na Internet.

Os objectos protegidos são divididos em três grupos:

- Ficheiros, dados pessoais, parâmetros de acesso a diferentes recursos (nomes de utilizador e passwords), informação sobre cartões bancários, etc. A protecção destes objectos é fornecida pelo Antivírus de Ficheiros e pela Defesa Proactiva.

- As aplicações instaladas no seu computador e os objectos do sistema operativo. A protecção destes objectos é fornecida pelo Antivírus de E-mail, Antivírus de Internet, Antivírus de MI e Defesa Proactiva.

- Actividades on-line: utilização de sistemas de pagamento on-line, protecção dos e-mails contra spam e vírus, etc. A protecção destes objectos é fornecida pelo Antivírus de E-mail, Antivírus de Internet, Antivírus de MI e Anti-Phishing.

ASSISTENTES E FERRAMENTAS

Garantir a segurança do computador é uma tarefa complexa que requer o conhecimento das funcionalidades do sistema operativo e dos métodos utilizados para explorar as suas fraquezas. Para além disso, o volume e a diversidade de informações sobre a segurança do sistema dificultam a sua análise e processamento.

Para ajudar a resolver tarefas específicas no fornecimento da segurança do computador, o pacote do Kaspersky Anti-Virus inclui um conjunto de assistentes e ferramentas:

- O Assistente de Configuração do Navegador (ver página 122) analisa as configurações do navegador Microsoft Internet Explorer, avaliando em primeiro lugar a questão da segurança.
- O Assistente de Restauro do Sistema (ver página 123) elimina os vestígios da presença de objectos de software malicioso no sistema.
- O Assistente de Limpeza de vestígio de actividade (ver página 124) procura e elimina rastreios de actividades do utilizador no sistema e nas configurações do sistema operativo, os quais poderiam permitir a recolha de informações sobre as actividades do utilizador.
- O Disco de Recuperação (ver página 120) foi concebido para verificar e desinfectar computadores compatíveis com x86 que foram infectados. A aplicação deve ser utilizada quando a infecção atinge um nível em que se considera ser impossível desinfectar o computador através de aplicações antivírus ou utilitários de remoção de software malicioso.
- A Verificação de Vulnerabilidade (ver página 83) executa diagnósticos do computador e procura vulnerabilidades no sistema operativo e nas aplicações de utilizador instaladas no computador.
- O Teclado Virtual (ver página 119) impede a intercepção dos dados inseridos através do teclado.

FUNCIONALIDADES DE SUPORTE DO PROGRAMA

O Kaspersky Anti-Virus inclui uma série de funcionalidades de suporte. Estas foram concebidas para manter a aplicação actualizada, para expandir as capacidades da aplicação e para o assistir enquanto a utiliza.

Ficheiros de dados e relatórios

Durante o funcionamento da aplicação, é criado um relatório para cada componente de protecção, tarefa de verificação ou tarefa de actualização da aplicação. Os relatórios contêm informação sobre actividades executadas e resultados das operações. Através destes, poderá obter informação detalhada sobre como funcionam as componentes do Kaspersky Anti-Virus. Se surgirem problemas, poderá enviar os relatórios à Kaspersky Lab para os nossos especialistas poderem estudar a situação em maior detalhe e ajudá-lo com a maior rapidez possível.

O Kaspersky Anti-Virus move todos os ficheiros suspeitos de serem perigosos para uma área de armazenamento especial denominada de *Quarentena*. Aqui são guardados na forma encriptada para evitar a infecção do computador. Pode fazer uma verificação de vírus nestes objectos, restaurá-los para a sua localização original, apagá-los ou adicionar, por si próprio, os ficheiros à Quarentena. Após terminar a verificação, todos os ficheiros, que se considere não estarem infectados, são automaticamente restaurados para a sua localização original.

A *Cópia de Segurança* guarda cópias de objectos desinfectados e apagados pelo Kaspersky Anti-Virus. Estas cópias são criadas caso seja necessário restaurar os ficheiros ou informação sobre a sua infecção. As cópias de segurança dos ficheiros são também guardadas na forma encriptada para evitar mais infecções.

Pode restaurar um ficheiro do armazenamento de cópias de segurança para a sua localização original ou apagar uma cópia.

Licença

Ao comprar o Kaspersky Anti-Virus, você entra num contrato de licença com a Kaspersky Lab que regula o uso da aplicação, assim como o seu acesso às actualizações da base de dados da aplicação e ao Suporte Técnico durante um período de tempo especificado. Os termos de uso e outras informações necessárias para a funcionalidade completa da aplicação são fornecidas numa licença.

Ao utilizar a função **Licença**, você pode obter informação detalhada sobre a sua licença actual, comprar uma nova licença ou renovar a licença existente.

Suporte

Todos os utilizadores registados do Kaspersky Anti-Virus podem beneficiar do nosso Serviço de Suporte Técnico. Para mais detalhes sobre as condições do serviço, utilize a opção **Suporte**.

Se seguir as ligações, pode aceder ao fórum de utilizadores dos produtos da Kaspersky Lab, enviar um relatório de erro ao Suporte Técnico ou fornecer informação de retorno sobre a aplicação, preenchendo um formulário especial on-line.

Também pode contactar o Suporte Técnico on-line e aceder aos Serviços de Arquivo Pessoal para Utilizadores. Os nossos funcionários terão todo o prazer em prestar-lhe suporte, por telefone, para o Kaspersky Anti-Virus.

INSTALAR O KASPERSKY ANTI-VIRUS

O Kaspersky Anti-Virus é instalado de forma interactiva, através do Assistente de Instalação.

Recomenda-se que feche todas as aplicações em execução antes de continuar com a instalação.

Para instalar o Kaspersky Anti-Virus no seu computador, execute o ficheiro de instalação (ficheiro com a extensão .exe) a partir do CD do produto.

Instalar o Kaspersky Anti-Virus a partir do ficheiro de instalação transferido da Internet é idêntico a instalar a aplicação a partir do CD.

Depois disso, tentar-se-á localizar o pacote de instalação do Kaspersky Anti-Virus (ficheiro com a extensão .msi) e, se o pacote for encontrado, tentar-se-á procurar uma versão mais recente nos servidores da Kaspersky Lab na Internet. Se não for encontrado o ficheiro do pacote de instalação, ser-lhe-á pedido para o transferir. Quando a transferência estiver concluída, iniciar-se-á a instalação do Kaspersky Anti-Virus. Se a transferência for cancelada, a instalação da aplicação continuará no modo padrão.

O programa de instalação é implementado como um assistente padrão do Windows. Cada janela contém um conjunto de botões para controlar o processo de instalação. De seguida, é apresentada uma breve descrição das suas funções:

- **Seguinte** – aceitar a acção e avançar para o próximo passo do processo de instalação.
- **Anterior** – voltar ao passo anterior do processo de instalação.
- **Cancelar** – cancelar a instalação.
- **Concluir** – concluir o procedimento de instalação da aplicação.

Vamos analisar em maior detalhe cada um dos passos do procedimento de instalação.

NESTA SECÇÃO:

Passo 1. Procurar uma versão mais recente da aplicação 21

Passo 2. Verificar se o sistema satisfaz os requisitos de instalação 21

Passo 3. Seleccionar o tipo de instalação 21

Passo 4. Visualizar o Contrato de Licença 22

Passo 5. Declaração de Recolha de Dados do Kaspersky Security Network 22

Passo 6. Seleccionar a pasta de instalação 22

Passo 7. Seleccionar as componentes da aplicação a instalar 22

Passo 8. Utilizar configurações da aplicação guardadas numa instalação anterior 23

Passo 9. Procurar outras aplicações antivírus 23

Passo 10. Preparação final para a instalação 24

Passo 11. Concluir a instalação 24

PASSO 1. PROCURAR UMA VERSÃO MAIS RECENTE DA APLICAÇÃO

Antes da instalação, a aplicação procura uma versão mais recente do Kaspersky Anti-Virus nos servidores de actualização da Kaspersky Lab.

Se não for encontrada uma versão mais recente nos servidores de actualização da Kaspersky Lab, será executado o Assistente de Instalação da versão actual.

Se for encontrada uma versão mais recente do Kaspersky Anti-Virus nos servidores de actualização, ser-lhe-á perguntado se deseja transferir e instalá-la. Se a instalação da versão mais recente for cancelada, será executado o Assistente de Instalação da versão actual. Se decidir instalar a versão mais recente, os ficheiros de instalação serão distribuídos para o seu computador e o Assistente de Instalação será, automaticamente, iniciado.

PASSO 2. VERIFICAR SE O SISTEMA SATISFAZ OS REQUISITOS DE INSTALAÇÃO

Antes de instalar o Kaspersky Anti-Virus no seu computador, o Assistente irá verificar se o sistema operativo e os service packs satisfazem os requisitos do programa para a instalação. Também irá verificar se tem o software necessário e os direitos necessários para instalar o software.

Se alguma das condições não for satisfeita, será apresentada no ecrã a respectiva notificação. Neste caso, antes de instalar uma aplicação da Kaspersky Lab, recomenda-se que instale os service packs necessários, através do serviço Windows Update, e todas as aplicações necessárias.

PASSO 3. SELECCIONAR O TIPO DE INSTALAÇÃO

Se o seu sistema cumprir todos os requisitos e se não for encontrada nenhuma versão mais recente da aplicação nos servidores de actualização da Kaspersky Lab ou se você tiver cancelado a instalação dessa versão mais recente, será executado o Assistente de Instalação da versão actual do Kaspersky Anti-Virus no seu computador.

Neste passo da instalação, você pode seleccionar a opção de instalação do Kaspersky Anti-Virus que melhor se adequa à sua situação.

- *Instalação rápid***a**. Se esta opção for seleccionada (a caixa **Instalação personalizada** não está assinalada), a aplicação será totalmente instalada no seu computador com as configurações de protecção predefinidas recomendadas pela Kaspersky Lab. Depois de concluída a instalação, será iniciado o Assistente de Configuração da Aplicação (ver página 26).
- *Instalação personalizada*. Neste caso, (se a caixa **Instalação personalizada** estiver assinalada), ser-lhe-á pedido para: seleccionar as componentes da aplicação que deseja instalar, especificar a pasta onde a aplicação será instalada e ainda activar e configurar a aplicação com um assistente especial.

Se seleccionar a primeira opção, o Assistente de Instalação da Aplicação dar-lhe-á a opção de visualizar o Contrato de Licença e a Declaração de recolha de dados do Kaspersky Security Network. Depois disso, a aplicação será instalada no seu computador.

Se seleccionar a segunda opção, ser-lhe-á pedido para introduzir ou confirmar determinados dados em cada passo da instalação.

Para continuar a instalação, clique no botão **Seguinte**. Para cancelar a instalação, clique no botão **Cancelar**.

PASSO 4. VISUALIZAR O CONTRATO DE LICENÇA

Neste passo, deve visualizar o Contrato de Licença que está a ser concluído entre você e a Kaspersky Lab.

Por favor, leia o contrato com atenção e se concordar com todos os termos do mesmo, clique no botão **Aceito**.
A instalação da aplicação continuará.

Para cancelar a instalação, clique no botão **Cancelar**.

PASSO 5. DECLARAÇÃO DE RECOLHA DE DADOS DO KASPERSKY SECURITY NETWORK

Neste passo, ser-lhe-á dada a opção de participar no programa Kaspersky Security Network. Participar no programa consiste em enviar à Kaspersky Lab: informação sobre novas ameaças detectadas no seu computador, o número de ID único atribuído ao seu computador pelo Kaspersky Anti-Virus, assim como informação sobre o sistema. Nesse processo, a Kaspersky Lab garante que os dados de privacidade não serão revelados.

Visualizar a Declaração de Recolha de Dados do Kaspersky Security Network. Se concordar com todos os termos do mesmo, assinale a caixa **Eu aceito os termos de participação no Kaspersky Security Network**.

Clique no botão **Seguinte**. A instalação irá continuar.

PASSO 6. SELECCIONAR A PASTA DE INSTALAÇÃO

Este passo do Assistente de Instalação só está disponível se a instalação personalizada da aplicação estiver em execução (ver secção "Passo 3. Seleccionar o tipo de instalação" na página 21).

Neste passo da instalação, ser-lhe-á pedido que especifique a pasta onde o Kaspersky Anti-Virus será instalado. O caminho predefinido é:

- **<drive> \ Program Files \ Kaspersky Lab \ Kaspersky Anti-Virus 2010** – para sistemas 32-bit.
- **<drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Anti-Virus 2010** – para sistemas 64-bit.

Pode especificar uma pasta diferente, clicando no botão **Procurar** e seleccionando a pasta na janela padrão de selecção da pasta ou inserindo o caminho da mesma no respectivo campo de registo.

Por favor, note que se inserir, manualmente, o caminho completo para a pasta de instalação, este não deve exceder os 200 caracteres e não deve conter caracteres especiais.

Para continuar a instalação, clique no botão **Seguinte**.

PASSO 7. SELECCIONAR AS COMPONENTES DA APLICAÇÃO A INSTALAR

Este passo do Assistente de Instalação só está disponível se a instalação personalizada da aplicação estiver em execução (ver secção "Passo 3. Seleccionar o tipo de instalação" na página 21).

Se a instalação personalizada estiver seleccionada, você deve especificar as componentes do Kaspersky Anti-Virus que deseja instalar no seu computador. Por defeito, todas as componentes do Kaspersky Anti-Virus são seleccionadas para instalação, incluindo componentes de protecção, tarefas de verificação e tarefas de actualização.

Para decidir quais as componentes que não deseja instalar, veja a informação resumida sobre cada componente. Para o fazer, seleccione a componente na lista e leia a informação sobre a mesma no campo por baixo. A informação inclui uma breve descrição do objectivo da componente e o espaço de disco necessário para a sua instalação.

Para cancelar a instalação de uma componente, abra o menu de atalho, clicando no ícone junto ao nome da componente, e seleccione o item **Este recurso ficará indisponível**. Note que se cancelar a instalação de uma componente, não será protegido contra uma série de programas perigosos.

Para seleccionar uma componente para a instalação, abra o menu de atalho, clicando no ícone junto ao nome da componente, e seleccione o item **Este recurso será instalado no disco rígido local**.

Depois de terminar de seleccionar as componentes a instalar, clique no botão **Seguinte**. Para regressar à lista predefinida de componentes a instalar, clique no botão **Repor**.

PASSO 8. UTILIZAR CONFIGURAÇÕES DA APLICAÇÃO GUARDADAS NUMA INSTALAÇÃO ANTERIOR

Neste passo, ser-lhe-á pedido que decida se deseja utilizar as definições de protecção e bases de dados da aplicação no seu trabalho futuro, caso estas tenham sido guardadas no seu computador depois de remover a versão anterior do Kaspersky Anti-Virus.

Vamos analisar em maior detalhe sobre como activar as funcionalidades acima descritas.

Se a versão anterior (compilação) do Kaspersky Anti-Virus esteve instalada no seu computador e você guardou as bases de dados da aplicação depois de remover essa versão, então pode integrá-las na versão que está a instalar. Para o fazer, assinale a caixa ☑ **Bases de dados da aplicação**. As bases de dados da aplicação incluídas no pacote de instalação não serão copiadas para o seu computador.

Para utilizar as definições de protecção que configurou numa versão anterior e que guardou no seu computador, assinale a caixa ☑ **Configurações operacionais da aplicação**.

PASSO 9. PROCURAR OUTRAS APLICAÇÕES ANTIVÍRUS

Neste passo, o assistente procura outros programas antivírus, incluindo outros programas da Kaspersky Lab, que podem entrar em conflito com o Kaspersky Anti-Virus.

Se forem detectadas aplicações antivírus no seu computador, as mesmas serão listadas no ecrã. Ser-lhe-á pedido que os desinstale antes de continuar com a instalação.

Por baixo da lista de aplicações antivírus detectadas, pode seleccionar o modo de eliminação (automático ou manual).

Se a versão de 2009 da aplicação da Kaspersky Lab estiver incluída na lista de aplicações antivírus detectadas, recomenda-se que guarde o ficheiro da chave utilizado por esta aplicação quando a remover manualmente. Poderá utilizar este ficheiro com uma versão actualizada da aplicação. Também se recomenda que guarde os objectos da Quarentena e da Cópia de Segurança. Estes objectos serão, automaticamente, colocados na Quarentena da versão actualizada do Kaspersky Anti-Virus e poderá continuar a trabalhar com os mesmos.

Se a versão de 2009 da aplicação for automaticamente removida, a informação sobre a activação será guardada pela aplicação e será utilizada durante a instalação da versão de 2010.

Para continuar a instalação, clique no botão **Seguinte**.

PASSO 10. PREPARAÇÃO FINAL PARA A INSTALAÇÃO

Este passo conclui a preparação para a instalação do Kaspersky Anti-Virus no seu computador.

Na instalação inicial e personalizada (ver secção "Passo 3. Seleccionar o tipo de instalação" na página 21) da aplicação, recomenda-se que não desmarque a caixa **Proteger o processo de instalação**. Se ocorrerem erros durante a instalação da aplicação, a activação desta protecção permitir-lhe-á efectuar um procedimento correcto de reversão da instalação. Quando voltar a tentar a instalação, recomendamos que desmarque esta caixa.

Se a aplicação estiver a ser instalada de forma remota, através do *Windows Remote Desktop*, recomenda-se que desmarque a caixa **Proteger o processo de instalação**. Se esta caixa estiver assinalada, o procedimento de instalação pode ser incorrectamente executado ou pode não ser concluído.

Para continuar a instalação, clique no botão **Instalar**.

Ao instalar as componentes do Kaspersky Anti-Virus, as quais interceptam o tráfego de rede, as actuais ligações de rede serão interrompidas. A maioria das ligações terminadas serão restauradas após uma pausa.

PASSO 11. CONCLUIR A INSTALAÇÃO

A janela **Instalação concluída** contém informação sobre a conclusão da instalação do Kaspersky Anti-Virus no seu computador.

O próximo passo é configurar a aplicação para garantir a máxima protecção da informação armazenada no seu computador. O Assistente de Configuração (ver secção "Assistente de Configuração da Aplicação" na página 26) ajudá-lo-á a configurar o Kaspersky Anti-Virus de forma rápida e adequada.

Depois, clique no botão **Seguinte** para aceder à configuração da aplicação.

COMO COMEÇAR

Um dos principais objectivos da Kaspersky Lab, ao criar o Kaspersky Anti-Virus, foi o de fornecer a configuração óptima da aplicação. Isso permite que os utilizadores com qualquer nível de conhecimentos informáticos garantam a protecção do seu computador logo após a instalação, sem desperdiçar o seu tempo precioso nas definições.

Para a conveniência do utilizador, procurámos integrar as etapas de configuração preliminar na interface do Assistente de Configuração da Aplicação (ver secção "Assistente de Configuração da Aplicação" na página 26) que se inicia com a finalização do procedimento de instalação. Ao seguir as instruções do assistente, você poderá activar o Kaspersky Anti-Virus, alterar as definições de actualização, restringir o acesso à aplicação com uma password e editar outras configurações.

O seu computador pode estar infectado com software malicioso antes do Kaspersky Anti-Virus ser instalado. Para detectar software malicioso, execute a verificação completa do computador.

Como resultado da operação do software malicioso ou de falhas do sistema, as configurações do seu computador podem ser corrompidas. Execute a tarefa de verificação de vulnerabilidades (ver secção "Verificação de vulnerabilidades no computador" na página 30) para detectar vulnerabilidades existentes em software instalado e anomalias nas configurações do sistema.

No momento de instalação da aplicação, as bases de dados incluídas no pacote de instalação podem estar obsoletas. Inicie a actualização da aplicação, caso esta não tenha sido efectuada pelo assistente de configuração ou de forma automática logo após a instalação da aplicação.

A componente Anti-Spam incluída no pacote do Kaspersky Anti-Virus utiliza um algoritmo de auto-aprendizagem para detectar mensagens indesejadas. Execute o Assistente de Treino do Anti-Spam para configurar a forma como a componente trabalha com a sua correspondência.

Depois de concluir as acções acima descritas, o Kaspersky Anti-Virus estará pronto para funcionar. Para avaliar o nível de protecção do seu computador, utilize o Assistente de Gestão de Segurança.

NESTA SECÇÃO:

Assistente de Configuração da Aplicação 26

Actualizar a aplicação 29

Verificação de vírus no computador 30

Verificação de vulnerabilidades no computador 30

Gerir a licença 31

Subscrição para a renovação automática da licença 31

Participar no Kaspersky Security Network 32

Gestão de Segurança 33

Estado de protecção 35

Pausar a protecção 35

ASSISTENTE DE CONFIGURAÇÃO DA APLICAÇÃO

O Assistente de Configuração da aplicação é iniciado após a instalação estar concluída. Foi concebido para o ajudar a configurar as definições iniciais do Kaspersky Anti-Virus, com base nas características e tarefas do seu computador.

A interface do Assistente de Configuração consiste numa série de passos em janelas, entre as quais pode navegar, utilizando o botão **Anterior** e a ligação **Seguinte**, ou fechar através do botão **Cancelar**.

DISCUSSÃO DETALHADA DOS PASSOS DO ASSISTENTE

Passo 1. Activar a aplicação 26

Passo 2. Seleccionar um modo de protecção 28

Passo 3. Configurar as actualizações da aplicação 28

Passo 4. Restringir o acesso à aplicação 29

Passo 5. Seleccionar ameaças detectáveis 29

Passo 6. Fechar o Assistente 29

PASSO 1. ACTIVAR A APLICAÇÃO

O procedimento de activação consiste em registar uma licença, instalando um ficheiro da chave. Com base na licença, a aplicação irá determinar os privilégios existentes e calcular o respectivo prazo de utilização.

O ficheiro da chave contém a informação de assistência necessária para que todas as funcionalidades do Kaspersky Anti-Virus funcionem, assim como dados adicionais:

- informação de suporte (quem presta o serviço de suporte e onde pode ser obtido);
- nome e número do ficheiro de chave e a data de validade da licença.

Vai precisar de uma ligação à Internet para activar a aplicação.

Para obter um ficheiro da chave na fase de activação, você deve ter um código de activação. O código de activação é fornecido quando adquirir a aplicação. Você tem as seguintes opções para activar o Kaspersky Anti-Virus:

- **Activar licença comercial**. Seleccione esta opção de activação se tiver adquirido uma versão comercial da aplicação e lhe tiver sido fornecido um código de activação. Pode usar este código para obter um ficheiro da chave que lhe dá acesso a todas as funcionalidades da aplicação durante todo o período da licença.
- **Activar licença de avaliação**. Use esta opção de activação se desejar instalar a versão de avaliação da aplicação, antes de tomar a decisão de comprar uma versão comercial. Ser-lhe-á fornecido um ficheiro de chave gratuito e válido durante um período especificado no contrato de licença da versão de avaliação.
- **Activar mais tarde**. Se seleccionar esta opção, a etapa de activação do Kaspersky Anti-Virus será ignorada. A aplicação será instalada no seu computador e você terá acesso a todas as funcionalidades do programa, excepto as actualizações (imediatamente a seguir à instalação, só estará disponível uma actualização da aplicação). A opção **Activar mais tarde** apenas estará disponível na primeira inicialização do Assistente de Activação, imediatamente após a instalação da aplicação.

Se o Kaspersky Anti-Virus tiver sido instalado e depois removido com a informação de activação guardada, este passo será ignorado. Neste caso, o Assistente de Configuração receberá, automaticamente, informação sobre a licença existente, a qual será apresentada na janela do assistente (ver página 27).

VEJA TAMBÉM:

Activar a versão comercial 27

Activar a versão de avaliação..... 27

Concluir a activação 27

ACTIVAR A VERSÃO COMERCIAL

Se seleccionar esta opção, a aplicação será activada a partir de um servidor da Kaspersky Lab que requer uma ligação à Internet.

A activação é efectuada, inserindo um código de activação que recebeu por e-mail quando adquiriu o Kaspersky Anti-Virus através da Internet. Se adquiriu a aplicação numa caixa (versão a retalho), o código de activação será impresso na face interior da capa do envelope do disco ou por baixo da camada protectora do autocolante na face interior da caixa do DVD.

O código de activação é uma sequência de números separados por hífenes em quatro grupos de cinco símbolos sem espaços. Por exemplo, 11111-11111-11111-11111. Note que o código de activação tem ser inserido em caracteres latinos.

O Assistente de Activação estabelece ligação com o servidor de activação da Kaspersky Lab na Internet, e envia o seu código de activação, após o qual o código é verificado. Se o código de activação passar na verificação com sucesso, o Assistente receberá um ficheiro da chave que será então automaticamente instalado. O processo de activação é concluído, acompanhado de uma janela com informação detalhada sobre a licença adquirida.

Se activar a subscrição, a informação sobre o estado de subscrição também estará disponível, para além da informação acima mencionada (ver secção "Subscrição para a renovação automática da licença" na página 31).

Se o código de activação não passar na verificação, você verá a mensagem correspondente no ecrã. Neste caso, deve contactar o fornecedor do software, ao qual você adquiriu o Kaspersky Anti-Virus, para solicitar informação.

Se for excedido o número de activações com o código de activação, surgirá o aviso correspondente no ecrã. O processo de activação será interrompido e aplicação dar-lhe-á a opção de contactar o Serviço de Suporte da Kaspersky Lab.

Se ocorrerem erros ao ligar a um servidor de activação e se você não conseguir obter um ficheiro da chave, por favor contacte o Serviço de Suporte Técnico.

ACTIVAR A VERSÃO DE AVALIAÇÃO

Use esta opção de activação se desejar instalar a versão de avaliação do Kaspersky Anti-Virus, antes de tomar a decisão de comprar uma versão comercial. Ser-lhe-á fornecido um ficheiro de chave gratuito e válido durante um período especificado no contrato de licença da versão de avaliação. Quando a licença de avaliação expirar, esta não pode ser activada pela segunda vez.

Se ocorrerem erros ao ligar a um servidor de activação e se você não conseguir obter um ficheiro da chave, por favor contacte o Serviço de Suporte Técnico.

CONCLUIR A ACTIVAÇÃO

O Assistente de Activação irá informá-lo de que o Kaspersky Anti-Virus foi activado com sucesso. Para além disso, também será fornecida informação sobre a licença: tipo de licença (comercial, avaliação, etc.), data de validade e o número de anfitriões para a licença.

Se activar a subscrição, será apresentada a informação sobre o estado de subscrição, em vez da data de validade da chave (ver secção "Subscrição para a renovação automática da licença" na página 31).

PASSO 2. SELECCIONAR UM MODO DE PROTECÇÃO

Seleccione o modo de protecção fornecido pelo Kaspersky Anti-Virus.

Estão disponíveis dois modos:

- *Automático*. Se ocorrer algum evento importante, o Kaspersky Anti-Virus irá executar, automaticamente, a acção recomendada pelos especialistas da Kaspersky Lab. Assim que for detectada uma ameaça, a aplicação tentará desinfectar o objecto e, se não for possível, irá apagá-lo. Os objectos suspeitos serão ignorados sem serem processados. Para informar o utilizador sobre novos eventos, são utilizadas mensagens de pop-up.

- *Interactivo*. Neste modo, a aplicação reage aos eventos da forma que você especificar. Assim que ocorrer um evento que requer a sua atenção, a aplicação exibe notificações (na página 132) que lhe dão a opção de seleccionar uma acção.

As notificações sobre a detecção de uma infecção activa serão apresentadas, independentemente do modo de protecção seleccionado.

PASSO 3. CONFIGURAR AS ACTUALIZAÇÕES DA APLICAÇÃO

Este passo do Assistente de Configuração da Aplicação será ignorado se tiver seleccionado o modo de instalação rápida. As definições da aplicação editadas neste passo terão atribuídos os valores predefinidos.

A qualidade da protecção do seu computador depende directamente da actualização regular das bases de dados e dos módulos da aplicação. Nesta janela, o Assistente de Configuração pede-lhe que seleccione o modo de actualização do Kaspersky Anti-Virus e que edite as definições de agendamento.

- **Actualizações automáticas**. O Kaspersky Anti-Virus verifica, em intervalos especificados, se existem pacotes de actualização na origem de actualização. A frequência dessa verificação pode aumentar durante surtos de vírus e diminuir quanto não existirem surtos. Se forem encontradas novas actualizações, o programa transfere-as e instala-as no computador. Este é o modo predefinido.

- **Actualizações agendadas** (o intervalo de tempo pode mudar dependendo das definições de agendamento). As actualizações serão automaticamente executadas com base no agendamento criado. Você pode alterar as definições de agendamento na janela que se abre quando clica no botão **Configuração**.

- **Actualizações manuais**. Se seleccionar esta opção, você executará as actualizações da aplicação manualmente.

Tenha em atenção que as bases de dados e os módulos da aplicação incluídos no pacote de instalação poderão estar desactualizados na altura em que instalar o Kaspersky Anti-Virus. Recomenda-se que obtenha as últimas actualizações do Kaspersky Anti-Virus. Para o fazer, clique no botão **Actualizar agora**. Neste caso, a aplicação irá transferir as actualizações necessárias a partir dos servidores de actualização e irá instalá-las no seu computador.

Se as bases de dados, incluídas no pacote de instalação, estiverem desactualizadas, o pacote de actualização pode ser extenso e isso pode implicar um tráfego adicional de Internet (até várias dezenas de Mb).

Se desejar aceder à edição das definições de actualização (ou seja, seleccionar o recurso a partir do qual serão transferidas as actualizações, a conta de utilizador usada para executar o processo de actualização e activar o serviço de distribuição de actualizações para uma origem local), clique no botão **Configuração** (ver secção "Actualização" na página 87).

PASSO 4. RESTRINGIR O ACESSO À APLICAÇÃO

Este passo do Assistente de Configuração do Kaspersky Anti-Virus será ignorado se tiver seleccionado o modo de instalação rápida. As definições da aplicação editadas neste passo terão atribuídos os valores predefinidos.

Uma vez que várias pessoas com diferentes níveis de conhecimentos informáticos poderão usar um computador pessoal e uma vez que os programas maliciosos podem desactivar a protecção, você tem a opção de proteger o acesso ao Kaspersky
Anti-Virus através de uma password. A utilização de uma password pode proteger a aplicação de tentativas não autorizadas para desactivar a protecção ou para alterar as definições do Kaspersky Anti-Virus.

Para activar a protecção por password, assinale a caixa ☑ **Activar protecção por password** e preencha os campos **Nova password** e **Confirmar nova password**.

Por baixo, especifique a área à qual pretende aplicar a protecção por password:

- ☑ **Configuração das definições da aplicação** – a password será solicitada quando o utilizador tentar guardar as alterações às definições do Kaspersky Anti-Virus.
- ☑ **Ao sair da aplicação** – a password será solicitada quando o utilizador tentar sair da aplicação.

PASSO 5. SELECCIONAR AMEAÇAS DETECTÁVEIS

Este passo do Assistente de Configuração da Aplicação será ignorado se tiver seleccionado o modo de instalação rápida. As definições da aplicação editadas neste passo terão atribuídos os valores predefinidos.

Nesta etapa, pode seleccionar a categoria de ameaças que o Kaspersky Anti-Virus irá detectar. O Kaspersky Anti-Virus detecta sempre os programas que são capazes de danificar o seu computador, incluindo vírus, worms e Trojans.

PASSO 6. FECHAR O ASSISTENTE

A última janela do Assistente irá informá-lo de que a instalação da aplicação foi concluída com sucesso. Para começar a trabalhar com o Kaspersky Anti-Virus, certifique-se de que a caixa ☑ **Iniciar o Kaspersky Anti-Virus** está assinalada e clique no botão **Concluir**.

ACTUALIZAR A APLICAÇÃO

Vai precisar de uma ligação à Internet para actualizar o Kaspersky Anti-Virus.

O pacote de instalação do Kaspersky Anti-Virus inclui as bases de dados, as quais contêm assinaturas de ameaças. Na altura em que o Kaspersky Anti-Virus é instalado, as bases de dados podem já estar obsoletas, uma vez que a Kaspersky Lab actualiza regularmente as bases de dados e os módulos da aplicação.

Quando o Assistente de Configuração da Aplicação estiver activo, você pode seleccionar o modo de execução da actualização (ver secção "Passo 3. Configurar as actualizações da aplicação" na página 28). Por defeito, o Kaspersky Anti-Virus verifica, automaticamente, a existência de actualizações nos servidores de actualização da Kaspersky Lab. Se o servidor contiver novas actualizações, o Kaspersky Anti-Virus irá transferi-las e instalá-las em modo silencioso.

Se as bases de dados, incluídas no pacote de instalação, estiverem desactualizadas, o pacote de actualização pode ser extenso e isso pode implicar um tráfego adicional de Internet (até várias dezenas de Mb).

Para manter a protecção do seu computador actualizada, recomenda-se que actualize o Kaspersky Anti-Virus imediatamente após a instalação.

Para actualizar por si próprio o Kaspersky Anti-Virus, execute as seguintes acções:

1. Abra a janela principal da aplicação.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Iniciar actualização**.

VERIFICAÇÃO DE VÍRUS NO COMPUTADOR

Os criadores de software malicioso fazem todos os esforços para esconderem as acções dos seus programas e, por isso, você pode não detectar a presença de programas maliciosos no seu computador.

Depois do Kaspersky Anti-Virus ser instalado, este executa automaticamente a tarefa de **Verificação Rápida** no seu computador. Esta tarefa procura e neutraliza programas prejudiciais existentes nos objectos que são carregados quando o sistema operativo é iniciado.

Os especialistas da Kaspersky Lab também recomendam que execute a tarefa de **Verificação Completa**.

Para iniciar uma tarefa de verificação de vírus, execute as seguintes acções:

1. Abra a janela principal da aplicação.
2. Na parte esquerda da janela, seleccione a secção **Verificação**.
3. Clique no botão **Iniciar Verificação Completa** para iniciar a verificação.

VERIFICAÇÃO DE VULNERABILIDADES NO COMPUTADOR

As configurações do seu sistema operativo podem ser corrompidas por falhas do sistema ou por actividades de programas maliciosos. Para além disso, as aplicações de utilizador instaladas no seu computador podem conter vulnerabilidades que os intrusos podem usar para danificar o seu computador.

Para detectar e eliminar esses problemas, recomenda-se que execute a *tarefa de Verificação de Vulnerabilidade* (ver página 83) depois de instalar a aplicação. Durante a execução da tarefa é efectuada uma pesquisa de vulnerabilidades em aplicações instaladas, assim como de danos e anomalias nas configurações do sistema operativo e do navegador de Internet.

Para iniciar a tarefa de verificação de vulnerabilidades:

1. Abra a janela principal da aplicação.
2. Na parte esquerda da janela, seleccione a secção **Verificação**.
3. Clique no botão **Abrir janela de Verificação de Vulnerabilidade**.
4. Na janela que se abre, clique no botão **Iniciar Verificação de Vulnerabilidade**.

GERIR A LICENÇA

O Kaspersky Anti-Virus precisa de um ficheiro de chave válida para funcionar. É fornecido um ficheiro da chave, utilizando o código de activação obtido ao adquirir a aplicação. Este dá-lhe o direito de utilizar a aplicação a partir da data de activação. O ficheiro da chave contém informação sobre a licença: o tipo, a data de validade e o número de anfitriões.

Sem um ficheiro da chave, a não ser que tenha activado uma versão de avaliação da aplicação, o Kaspersky Anti-Virus funcionará no modo que permite apenas uma actualização. A aplicação não transferirá actualizações novas.

Se tiver activado uma versão de avaliação do programa, após terminar o período de avaliação, o Kaspersky Anti-Virus deixará de funcionar.

Quando a licença comercial expirar, a aplicação continuará a funcionar, mas não conseguirá actualizar as bases de dados. Tal como anteriormente, poderá analisar o seu computador em termos de vírus e utilizar as componentes de protecção, mas só utilizando as bases de dados que possuía quando a licença expirou. Não podemos garantir que fique protegido dos vírus que surjam depois da sua licença da aplicação expirar.

Para evitar a infecção do seu computador com novos vírus, recomendamos que prolongue a sua licença para o Kaspersky Anti-Virus. A aplicação notificá-lo-á duas semanas antes de a licença expirar. Durante algum tempo, será exibida uma mensagem adequada sempre que iniciar a aplicação.

A informação sobre a licença actualmente em uso é apresentada na janela **Gestor de licenças**: tipo de licença (comercial, comercial com subscrição, comercial com subscrição de protecção, avaliação), o número máximo de anfitriões, a data de validade e o número de dias restantes. A informação sobre a validade da licença não será apresentada se estiver instalada uma licença comercial com subscrição ou licença comercial com subscrição de protecção (ver secção "Subscrição para a renovação automática da licença" na página 31).

Para ver as disposições do contrato de licença da aplicação, clique no botão **Ver Contrato de Licença do Utilizador Final**. Para apagar o ficheiro da chave, clique no botão ✖ à direita da licença cujo ficheiro da chave deseja apagar. Para activar uma nova licença, clique no botão **Activar nova licença**.

Ao utilizar o botão **Comprar licença** (**Renovar licença**), pode proceder à aquisição (renovação) da licença na loja on-line da Kaspersky Lab.

A Kaspersky Lab tem regularmente ofertas com preços especiais para prolongar as licenças dos nossos produtos. Procure ofertas especiais no site da Kaspersky Lab, na secção **Products & Services** → **Sales and special offers**.

SUBSCRIÇÃO PARA A RENOVAÇÃO AUTOMÁTICA DA LICENÇA

A subscrição permite renovar a licença de forma automática. Para activar a subscrição, irá precisar de um código de activação que pode obter numa loja on-line quando adquirir o Kaspersky Anti-Virus.

No momento de activação da subscrição, se já tiver uma licença activada com prazo limitado, esta será substituída pela licença de subscrição. Para cancelar a subscrição, contacte a loja on-line onde comprou o Kaspersky Anti-Virus.

São utilizadas as seguintes opções para designar o estado de subscrição:

- *A ser definido*. O seu pedido para activar a subscrição ainda não foi processado (é necessário algum tempo para processar o pedido no servidor). O Kaspersky Anti-Virus funciona em modo de total funcionalidade. Se após um determinado período de tempo o pedido de subscrição não tiver sido processado, você receberá uma notificação de que a actualização do estado de subscrição não foi executada. Neste caso, as bases de dados da aplicação deixarão de ser actualizadas (para a licença com subscrição), assim como a protecção do computador deixará de ser executada (para a licença com subscrição de protecção).

- *Activada*. A subscrição foi activada sem prazo fixado ou por um determinado período de tempo (data de validade da subscrição está definida).

- *Renovada*. A subscrição foi renovada sem prazo fixado ou por um determinado período de tempo.

- *Erro*. Ocorreu um erro ao actualizar o estado de subscrição.
- *Expirou. Período de tolerância.* A subscrição expirou ou o prazo de renovação do estado expirou. Se o prazo de renovação do estado tiver expirado, actualize o estado de subscrição manualmente. Se a subscrição tiver expirado, pode renová-la, contactando a loja on-line onde adquiriu o Kaspersky Anti-Virus. Para utilizar um código de activação diferente, primeiro deve apagar o ficheiro de chave para a subscrição que está actualmente a utilizar.
- *Expirou. Período de tolerância expirou.* A subscrição expirou ou o período de tolerância para a renovação da licença expirou. Por favor, contacte o seu fornecedor de subscrição para adquirir uma nova subscrição ou para renovar a subscrição existente.
- *Subscrição cancelada.* Você cancela a subscrição para a renovação automática da licença.
- *A renovação é necessária*. Por alguma razão, o estado de subscrição não foi actualizado a tempo. Use o botão **Actualizar o estado de subscrição** para actualizar o estado de subscrição.
- *Suspensa*. A subscrição para a renovação automática da licença foi suspensa.
- *Retomada*. A subscrição foi retomada.

Se o período de validade da subscrição tiver terminado, assim como o período de tolerância durante o qual a licença pode ser renovada (estado de subscrição – *Expirou*), o Kaspersky Anti-Virus irá notificá-lo sobre isso e deixará de tentar renovar a licença automaticamente. Para a licença com subscrição, a funcionalidade da aplicação será mantida, com excepção da função de actualização das bases de dados. Para a licença com subscrição de protecção, as bases de dados da aplicação não serão actualizadas, a protecção do computador não será executada, bem como as tarefas de verificação.

Se, por alguma razão, a licença não tiver sido renovada a tempo (estado de subscrição – *A renovação é necessária*), por exemplo porque o computador estava desligado durante todo o tempo em que a renovação da licença estava disponível, você pode renovar o estado manualmente. Até ao momento da renovação da subscrição, o Kaspersky Anti-Virus deixa de actualizar as bases de dados da aplicação (para a licença com subscrição), assim como deixa de executar a protecção do computador (para a licença com subscrição de protecção).

Enquanto estiver a utilizar a subscrição, não poderá utilizar outro código de activação para renovar a licença. Esta opção apenas estará disponível depois de a subscrição expirar (estado de subscrição – *Expirou*). Para renovar a licença, ser-lhe-á dado um período de tolerância, durante o qual a funcionalidade da aplicação será preservada.

Quando utiliza a subscrição e reinstala a aplicação no seu computador, precisará de voltar a activar o produto manualmente, através do código de activação que obteve quando comprou a aplicação.

Dependendo do fornecedor de subscrição, o conjunto de acções disponíveis para executar com a subscrição pode variar. Para além disso, o período de tolerância, quando a renovação da licença está disponível, não será fornecido por defeito.

PARTICIPAR NO KASPERSKY SECURITY NETWORK

Todos os dias surgem inúmeras ameaças novas a nível mundial. Para facilitar a recolha de estatísticas sobre novos tipos de ameaças, a sua origem e sobre como eliminá-las, a Kaspersky Lab convida-o a utilizar o serviço Kaspersky Security Network.

A utilização do Kaspersky Security Network envolve o envio das seguintes informações à Kaspersky Lab:

- Um identificador único atribuído ao seu computador pelo Kaspersky Anti-Virus, o qual caracteriza as configurações de hardware do seu computador e não contêm nenhuma outra informação.
- Informação sobre ameaças detectadas pelas componentes da aplicação. A estrutura e conteúdos da informação depende do tipo de ameaça detectada.
- Informação sobre o sistema: a versão do sistema operativo, pacotes de serviço instalados, serviços e controladores a serem transferidos, versões dos clientes de e-mail e dos navegadores de Internet, extensões do navegador, número da versão instalada da aplicação da Kaspersky Lab.

O Kaspersky Security Network também recolhe estatísticas avançadas, incluindo informação sobre:

- ficheiros executáveis e aplicações assinadas transferidas para o seu computador,
- aplicações em execução no seu computador.

Esta informação estatística é enviada assim que for concluída a actualização da aplicação.

A Kaspersky Lab garante que não é efectuada qualquer recolha ou distribuição de dados pessoais dos utilizadores no âmbito do Kaspersky Security Network.

Para configurar o envio de estatísticas:

1. Abra a janela de configuração da aplicação.
2. Seleccione a secção **Informação de Retorno** na parte esquerda da janela.
3. Assinale a caixa **Aceito participar no Kaspersky Security Network** para confirmar a sua participação no Kaspersky Security Network.

GESTÃO DE SEGURANÇA

O estado de protecção do computador indica problemas existentes na protecção do computador (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39), o qual é apresentado por alterações da cor do ícone do estado de protecção e do painel onde este ícone se encontra. Quando surgem problemas no sistema de protecção, recomenda-se que os corrija imediatamente.

Figura 1. Estado actual da protecção do computador

Pode ver a lista dos problemas ocorridos, a sua descrição e possíveis métodos de resolução, no separador **Estado** (ver figura abaixo). Pode seleccioná-lo, clicando no ícone de estado ou no painel onde este se encontra (ver figura acima).

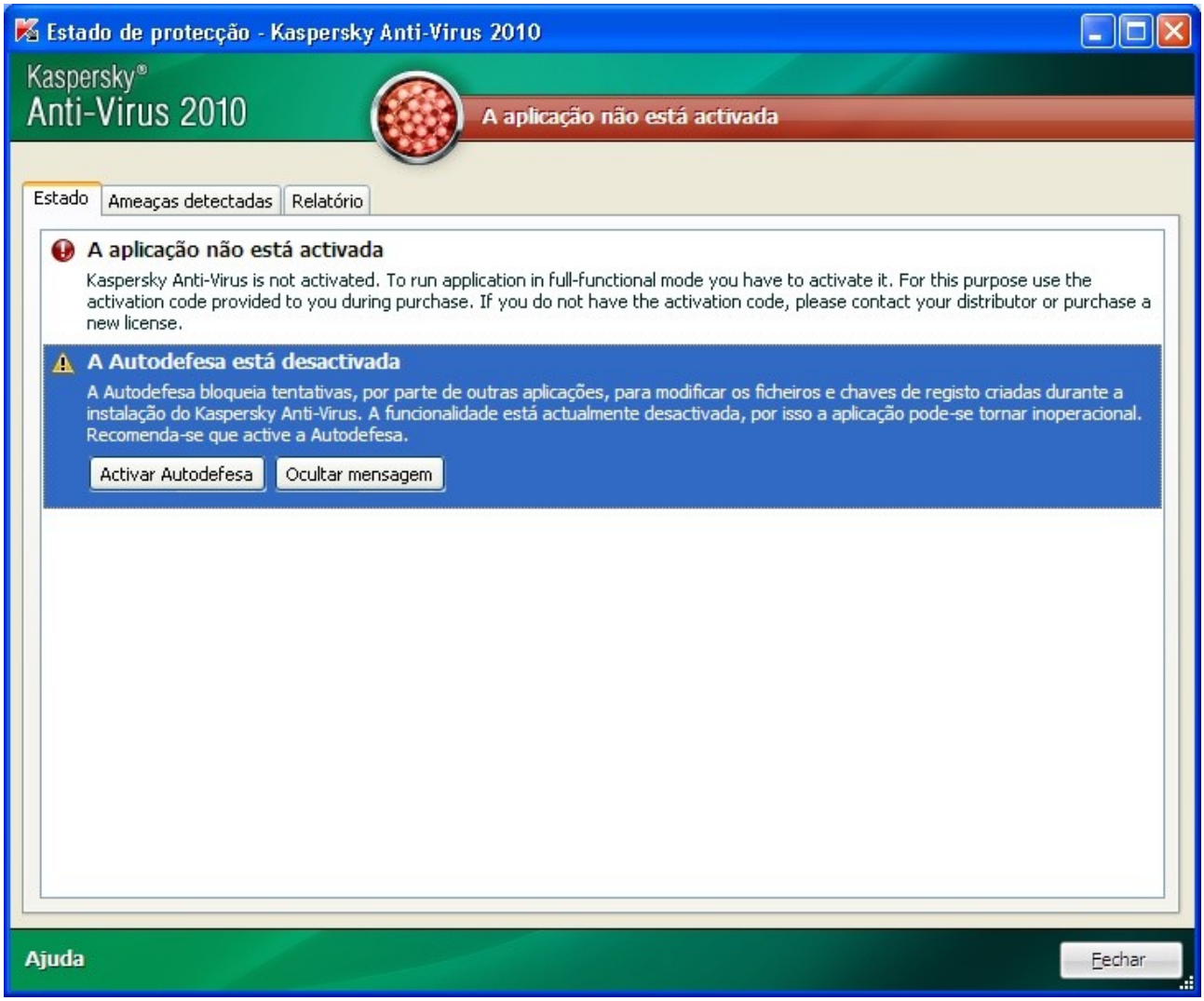

Estado de protecção - Kaspersky Anti-Virus 2010
Kaspersky®
Anti-Virus 2010
A aplicação não está activada
Estado
Ameaças detectadas
Relatório
A aplicação não está activada
Kaspersky Anti-Virus is not activated. To run application in full-functional mode you have to activate it. For this purpose use the activation code provided to you during purchase. If you do not have the activation code, please contact your distributor or purchase a new license.
A Autodefesa está desactivada
A Autodefesa bloqueia tentativas, por parte de outras aplicações, para modificar os ficheiros e chaves de registo criadas durante a instalação do Kaspersky Anti-Virus. A funcionalidade está actualmente desactivada, por isso a aplicação pode-se tornar inoperacional. Recomenda-se que active a Autodefesa.
Activar Autodefesa
Ocultar mensagem
Ajuda
Fechar

Figura 2. Resolver problemas de segurança

O separador apresenta a lista dos actuais problemas. Os problemas estão ordenados de acordo com a sua criticalidade: em primeiro, os problemas mais críticos (ou seja, com o ícone de estado vermelho), em segundo, os problemas menos críticos (com o ícone de estado amarelo) e, por último, as mensagens informativas. Para cada problema é fornecida uma descrição detalhada e estão disponíveis as seguintes acções:

- *Eliminar imediatamente*. Através dos respectivos botões, você pode começar a corrigir o problema, que é a acção recomendada.

- *Adiar a eliminação*. Se, por alguma razão, não puder eliminar o problema imediatamente, você pode adiar esta acção e voltar à mesma mais tarde. Para o fazer, clique no botão **Ocultar mensagem**.

  Note que esta opção não está disponível para os problemas graves. Esses problemas incluem, por exemplo, objectos maliciosos que não foram desinfectados, falhas de uma ou várias componentes ou a corrupção dos ficheiros do programa.

Para que as mensagens ocultadas voltem a aparecer na lista geral, assinale a caixa **Mostrar mensagens ocultadas**.

ESTADO DE PROTECÇÃO

O desempenho das componentes do Kaspersky Anti-Virus ou das tarefas de verificação de vírus é registado no relatório que contém informação resumida sobre o estado de protecção do computador. Nessa secção pode saber quantos objectos perigosos e suspeitos foram detectados pela aplicação e descobrir quais foram desinfectados, apagados ou colocados na quarentena.

O estado de protecção do computador (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39) avisa o utilizador sobre os objectos maliciosos detectados pela aplicação, alterando a cor do ícone do estado de protecção e do painel onde este ícone se encontra. Se forem detectados objectos maliciosos, a cor do ícone e do painel muda para vermelho. Neste caso, todas as novas ameaças devem ser imediatamente eliminadas.

Para ver informação sobre o estado de protecção do computador:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Relatório**.

Para eliminar problemas ocorridos na protecção do computador:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Relatório**.
3. Execute as acções necessárias no separador **Estado** da janela que se abre. Para que as mensagens ocultadas voltem a aparecer na lista geral, assinale a caixa **Mostrar mensagens ocultadas**.

Para executar uma acção sobre um objecto detectado:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Relatório**.
3. Na janela que se abre, no separador **Ameaças detectadas** seleccione o objecto desejado na lista e clique sobre o mesmo com o botão direito do rato para abrir o respectivo menu de contexto.
4. Seleccione a acção desejada no menu que se abre.

Para ver o relatório sobre o funcionamento das componentes de protecção:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Relatório**.
3. Na janela que se abre, seleccione o separador **Relatório**.

PAUSAR A PROTECÇÃO

Pausar a protecção significa desactivar, temporariamente, todas as componentes de protecção durante um determinado período de tempo.

Como resultado da desactivação temporária da protecção, todas as componentes de protecção serão pausadas. Isto será indicado por:

- ícone da aplicação inactivo (a cinzento) (ver secção "Ícone da área de notificação" na página 37) na área de notificação da barra de ferramentas;
- cor vermelha para o ícone de estado e o painel da janela principal da aplicação.

Se existiam ligações de rede estabelecidas no momento em que a protecção foi pausada, será apresentada uma notificação sobre a interrupção dessas ligações.

Para pausar a protecção do seu computador:

1. No menu de contexto da aplicação (ver secção "Menu de contexto" na página 38), seleccione o item **Pausar Protecção**.

2. Na janela **Pausar a protecção** que se abre, seleccione o intervalo de tempo após o qual a protecção deve ser retomada:

   - **Pausar durante <intervalo de tempo> –** a protecção será activada após um período de tempo especificado. Para seleccionar um intervalo de tempo, use o menu suspenso.

   - **Pausar até à reinicialização –** a protecção será activada após a reinicialização da aplicação ou após o reinício do sistema (desde que o Kaspersky Anti-Virus esteja configurado para se iniciar automaticamente com a inicialização do sistema).

   - **Pausar** – a protecção será activada somente depois de você a iniciar manualmente. Para activar a protecção, seleccione o item **Retomar protecção** a partir do menu de contexto da aplicação.

INTERFACE DA APLICAÇÃO

O Kaspersky Anti-Virus possui uma interface relativamente simples e fácil de utilizar. Esta secção discutirá as suas características básicas em detalhe.

O Kaspersky Anti-Virus possui extensões que estão integradas no Microsoft Office Outlook, The Bat!, Microsoft Internet Explorer, Microsoft Windows Explorer. As extensões aumentam as funcionalidades destes programas, uma vez através das suas interfaces é possível configurar as componentes da aplicação.

NESTA SECÇÃO:

Ícone da área de notificação 37

Menu de contexto 38

Janela principal do Kaspersky Anti-Virus 39

Notificações 41

Janela de configuração da aplicação 41

ÍCONE DA ÁREA DE NOTIFICAÇÃO

Logo após a instalação do Kaspersky Anti-Virus, o ícone da aplicação aparecerá na área de notificação da barra de tarefas do Microsoft Windows.

Este ícone é um indicador do funcionamento actual da aplicação. Também reflecte o estado de protecção e apresenta uma série de funções básicas executadas pela aplicação.

Se o ícone estiver activo (a cores), a protecção está completamente activada ou algumas das suas componentes estão a funcionar. Se o ícone estiver inactivo (a preto e branco), todas as componentes de protecção estão desactivadas.

O ícone do Kaspersky Anti-Virus altera-se dependendo da operação que está a ser executada:

- – está a ser verificado um e-mail;
- – o tráfego de Internet está a ser verificado;
- – a actualização das bases de dados e dos módulos da aplicação está a decorrer;
- – o computador precisa de ser reiniciado para aplicar as actualizações;
- – ocorreu uma falha no funcionamento de alguma componente da aplicação.

O ícone também permite o acesso aos elementos básicos da interface da aplicação: o menu de contexto (ver secção "Menu de contexto" na página 38) e a janela principal (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39).

O menu de contexto é aberto, clicando sobre o ícone da aplicação com o botão direito do rato.

Para abrir a janela principal do Kaspersky Anti-Virus, clique com o botão esquerdo do rato sobre o ícone da aplicação.

Se estiverem disponíveis notícias da Kaspersky Lab, o ícone aparecerá na área de notificação da barra de tarefas do Microsoft Windows. O texto das notícias pode ser aberto, clicando duas vezes sobre o respectivo ícone.

MENU DE CONTEXTO

Você pode executar tarefas básicas de protecção a partir do menu de contexto.

O qual contém os seguintes itens:

- **Actualização** – inicia as actualizações dos módulos e das bases de dados da aplicação e instala as actualizações no seu computador.
- **Verificação Completa** – inicia uma verificação completa do seu computador quanto à existência de objectos maliciosos. Serão verificados os objectos existentes em todas as unidades, incluindo meios de armazenamento removíveis.
- **Verificação de vírus** – selecciona objectos e inicia uma verificação de vírus. A lista predefinida contém vários objectos, tais como a pasta **Os Meus Documentos** e as caixas de e-mail. Pode alargar esta lista, seleccionando objectos para verificação e iniciar uma verificação de vírus.
- **Teclado virtual** – muda para o teclado virtual.
- **Kaspersky Anti-Virus** – abre a janela principal da aplicação (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39).
- **Configuração** – ver e configurar as definições da aplicação.
- **Activar** – aceder à activação do Kaspersky Anti-Virus. Para obter o estatuto de utilizador registado, tem de activar a sua aplicação. Este item do menu apenas está disponível se a aplicação não tiver sido activado.
- **Sobre** – apresenta uma janela com informação sobre a aplicação.
- **Pausar protecção / Retomar protecção** – activa ou desactiva temporariamente as componentes de protecção em tempo real. Esta opção do menu não afecta a execução das actualizações da aplicação ou das tarefas de verificação de vírus.
- **Sair** – fecha o Kaspersky Anti-Virus (quando esta opção é seleccionada, a aplicação será descarregada da memória RAM do computador).

Figura 3. Menu de contexto

Se estiver a decorrer uma tarefa de verificação de vírus, quando abre o menu de contexto, o respectivo nome e o estado de evolução (percentagem de conclusão) serão apresentados no menu de contexto. Ao seleccionar a tarefa, poderá aceder à janela principal que contém um relatório sobre os resultados actuais da sua execução.

JANELA PRINCIPAL DO KASPERSKY ANTI-VIRUS

A janela principal da aplicação pode ser dividida em três partes:

- A parte superior da janela indica o estado actual da protecção do seu computador.

Figura 4. Estado actual da protecção do computador

Existem três valores possíveis para o estado de protecção: cada um deles é indicado por uma determinada cor, semelhante aos semáforos do trânsito. A cor verde indica que a protecção do seu computador está no nível correcto, enquanto as cores amarelo e vermelho indicam que existem várias ameaças de segurança. Para além dos programas maliciosos, as ameaças incluem bases de dados da aplicação obsoletas, componentes de protecção desactivadas, a selecção de configurações de protecção mínimas, etc.

As ameaças de segurança tem de ser eliminadas assim que aparecem. Para obter informação detalhada sobre as ameaças e sobre como as eliminar rapidamente, aceda ao Assistente de Gestão de Segurança: clique no ícone de estado ou no painel onde este se encontra (ver fig. acima).

- A parte esquerda da janela permite um acesso rápido a qualquer das funções da aplicação, incluindo as tarefas de verificação de vírus e de actualização, etc.

Figura 5. Parte esquerda da janela principal

- A parte direita da janela contém información sobre a função da aplicação seleccionada na parte esquerda, permite configurar as respectivas definições, fornece ferramentas para executar tarefas de verificação de vírus, transferir actualizações, etc.

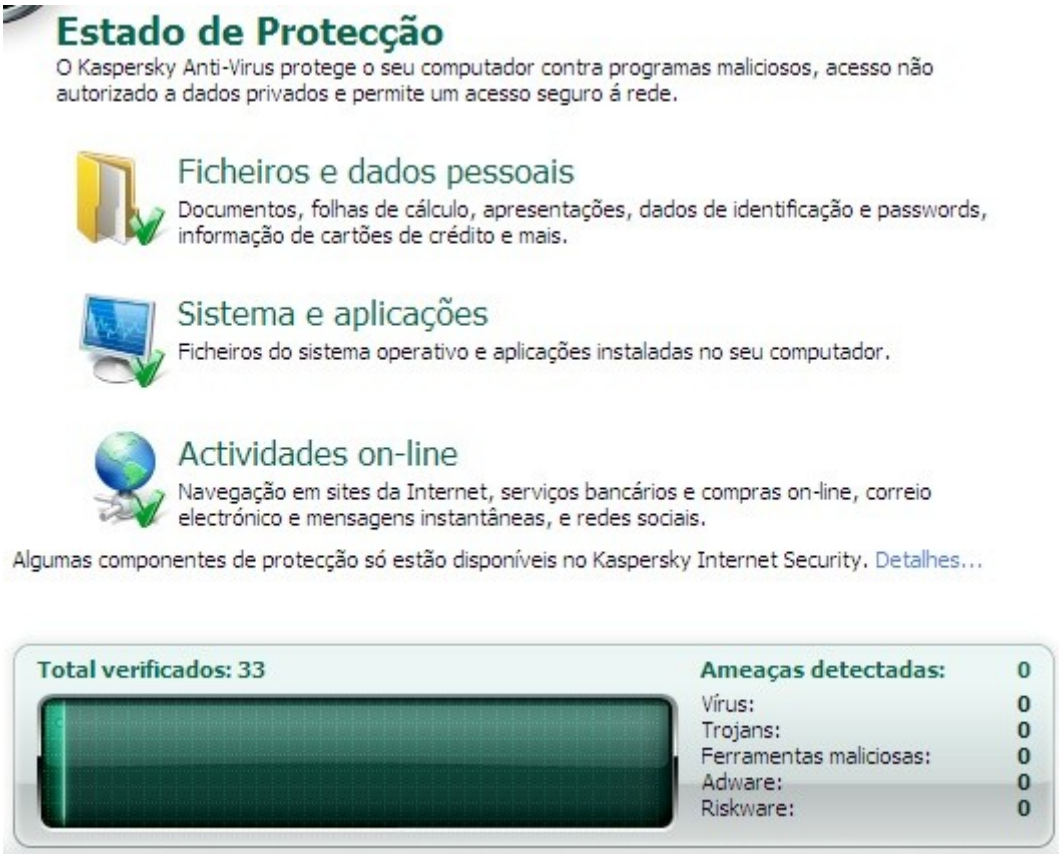

Estado de Protecção
O Kaspersky Anti-Virus protege o seu computador contra programas maliciosos, acesso não autorizado a dados privados e permite um acesso seguro á rede.
Ficheiros e dados pessoais
Documentos, folhas de cálculo, apresentações, dados de identificação e passwords, informação de cartões de crédito e mais.
Sistema e aplicações
Ficheiros do sistema operativo e aplicações instaladas no seu computador.
Actividades on-line
Navegação em sites da Internet, serviços bancários e compras on-line, correio electrónico e mensagens instantâneas, e redes sociais.
Algumas componentes de protecção só estão disponíveis no Kaspersky Internet Security. Detalhes...
Total verificados: 33
Ameaças detectadas: 0
Vírus: 0
Trojans: 0
Ferramentas maliciosas: 0
Adware: 0
Riskware: 0

Figura 6. Parte direita da janela principal

Também pode utilizar os seguintes botões e ligações:

- **Configuração** – para abrir a janela de configuração da aplicação (ver secção "Configuração das definições da aplicação" na página 93).
- **Quarentena** – para começar a trabalhar com objectos em quarentena.
- **Relatório** – para abrir a lista de eventos que ocorreram durante o funcionamento da aplicação.
- **Ajuda** – para abrir a ajuda do Kaspersky Anti-Virus.
- **Conta Kaspersky** – para abrir o arquivo pessoal do utilizador no site do serviço de Suporte Técnico.
- **Suporte** – para abrir a janela com información sobre o sistema e links para os recursos de información da Kaspersky Lab (site do serviço de Suporte Técnico, fórum).
- **Licença** – activação do Kaspersky Anti-Virus, prolongamento do período da licença.

Pode mudar a aparência do Kaspersky Anti-Virus, criando e utilizando vários gráficos e esquemas de cores.

NOTIFICAÇÕES

Se ocorrerem eventos no decurso do funcionamento do Kaspersky Anti-Virus, serão apresentadas notificações especiais no ecrã, sob a forma mensagens de popup, por cima do ícone da aplicação na barra de tarefas do Microsoft Windows.

Dependendo do nível de criticalidade do evento, no que respeita à segurança do computador, você pode receber os seguintes tipos de notificações:

- **Alarme**. Ocorreu um evento crítico. Por exemplo, foi detectado um vírus ou uma actividade perigosa no seu sistema. Deve decidir de imediato sobre como lidar com esta ameaça. Este tipo de notificações são destacadas a vermelho.

- **Aviso**. Ocorreu um evento potencialmente perigoso. Por exemplo, foram detectados no seu sistema ficheiros potencialmente infectados ou actividades suspeitas. Você deve decidir sobre o nível de perigo deste evento. Este tipo de notificações são destacadas a amarelo.

- **Informação**. Esta notificação fornece-lhe informação sobre eventos que não são críticos. As notificações de informação são destacadas a verde.

VEJA TAMBÉM:

Notificações.....132

JANELA DE CONFIGURAÇÃO DA APLICAÇÃO

A janela de configuração do Kaspersky Anti-Virus pode ser aberta a partir da janela principal (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39) ou a partir do menu de contexto (ver secção "Menu de contexto" na página 38). Para abrir esta janela, clique na ligação **Configuração** na parte superior da janela principal da aplicação ou seleccione a opção adequada no menu de contexto da aplicação.

A janela de configuração da aplicação consiste em duas partes:

- a parte esquerda da janela permite o acesso às funções do Kaspersky Anti-Virus, às tarefas de verificação de vírus, às actualizações, etc.;

- a parte direita da janela contém uma lista de configurações para a componente, tarefa, etc. seleccionada na parte esquerda da janela.

PROTECÇÃO DO SISTEMA DE FICHEIROS DO COMPUTADOR

O *Antivírus de Ficheiros* previne a infecção do sistema de ficheiros do computador. Este é carregado quando inicia o seu sistema operativo e é executado na memória RAM do seu computador, verificando todos os ficheiros abertos, guardados ou executados.

Por defeito, o Antivírus de Ficheiros apenas verifica ficheiros novos ou modificados. Um conjunto de definições, denominado de nível de segurança, determina as condições da verificação de ficheiros. Se o Antivírus de Ficheiros detectar uma ameaça, este irá executar a acção definida.

O nível de protecção de ficheiros e memória no seu computador é determinado pelo seguinte conjunto de definições:

- definições que criam o âmbito de protecção;
- definições que determinam o método de verificação;
- definições que determinam a forma como os ficheiros compostos são verificados (incluindo a verificação de ficheiros compostos extensos);
- definições que determinam o modo de verificação;
- definições que permitem pausar a componente de acordo com o agendamento ou durante o funcionamento das aplicações seleccionadas.

Os especialistas da Kaspersky Lab recomendam que não configure sozinho o Antivírus de Ficheiros. Na maioria dos casos, será suficiente alterar o nível de segurança. Para restaurar as predefinições do Antivírus de Ficheiros, seleccione um dos níveis de segurança.

Para alterar a configuração do Antivírus de Ficheiros:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Faça as alterações necessárias na configuração da componente.

NESTA SECÇÃO:

Algoritmo de funcionamento da componente 43

Alterar o nível de segurança dos ficheiros e da memória 44

Alterar as acções a executar com objectos detectados 45

Criar um âmbito de protecção 45

Utilizar a Análise Heurística 46

Optimização da verificação 47

Verificação de ficheiros compostos 47

Verificar ficheiros compostos extensos 48

Alterar o modo de verificação 48

Tecnologia de verificação 49

Pausar a componente: criar um agendamento 49

Pausar a componente: criar uma lista de aplicações 50

Restaurar as predefinições de protecção 51

ALGORITMO DE FUNCIONAMENTO DA COMPONENTE

A componente *Antivírus de Ficheiros* é carregada quando inicia o seu sistema operativo e é executada na memória do seu computador, verificando todos os ficheiros abertos, guardados ou executados.

Por defeito, o Antivírus de Ficheiros apenas verifica ficheiros novos ou modificados, ou seja, ficheiros que foram adicionados ou modificados desde a última verificação. Os ficheiros são verificados de acordo com o seguinte algoritmo:

1. A componente intercepta o acesso a cada ficheiro tentado pelo utilizador ou por qualquer programa.
2. *Antivírus de Ficheiros verifica a base de dados das tecnologias iChecker e iSwift, procurando informação sobre o ficheiro interceptado, e determina se o ficheiro deve ou não ser verificado, com base na informação recolhida.*

São executadas as seguintes operações durante a verificação:

1. O ficheiro é analisado em termos da presença de vírus. Os objectos maliciosos são reconhecidos utilizando as bases de dados do Kaspersky Anti-Virus. A base de dados contém descrições de todos os programas maliciosos e ameaças conhecidos até à data e dos métodos para os processar.
2. Depois da análise, você tem à disposição as seguintes acções para o Kaspersky Anti-Virus:
   a. Se for detectado código malicioso no ficheiro, o Antivírus de Ficheiros bloqueia o ficheiro, cria uma cópia de segurança e tenta executar a desinfecção. Se o ficheiro for desinfectado com sucesso, o ficheiro fica novamente disponível. Se a desinfecção falhar, o ficheiro será apagado.
   b. Se for detectado código potencialmente malicioso num ficheiro (mas não houver certeza absoluta de que é malicioso), o ficheiro prosseguirá para a desinfecção e depois é enviado para a área de armazenamento especial, denominada Quarentena.
   c. Se não for descoberto nenhum código malicioso no ficheiro, o mesmo será imediatamente restaurado.

A aplicação irá notificá-lo quando for detectado um ficheiro infectado ou possivelmente infectado. Se for detectado um objecto infectado ou potencialmente infectado, será exibida no ecrã uma notificação a solicitar acções adicionais. Ser-lhe-ão dadas as seguintes opções:

- colocar o objecto na Quarentena, permitindo que a nova ameaça seja verificada e processada mais tarde, através das bases de dados actualizadas;
- apagar o objecto;
- ignorar o objecto, se tiver a certeza absoluta de que não é malicioso.

ALTERAR O NÍVEL DE SEGURANÇA DOS FICHEIROS E DA MEMÓRIA

O nível de segurança é definido como uma configuração predefinida das definições da componente Antivírus de Ficheiros. Os especialistas da Kaspersky Lab distinguem três níveis de segurança. A decisão sobre o nível de segurança a seleccionar tem de ser tomada pelo utilizador, com base nas condições de funcionamento e na situação actual. Terá a possibilidade de seleccionar uma das seguinte opções para o nível de segurança:

- **Elevado**. Se suspeita que o seu computador têm uma elevada probabilidade de ser infectado, seleccione este nível.
- **Recomendado**. Este nível permite um equilíbrio entre eficiência e segurança e é adequado para a maioria dos casos.
- **Baixo**. Se trabalha num ambiente protegido (por exemplo, uma rede empresarial com um sistema de segurança centralizado), o nível de segurança baixo pode ser adequado. Também pode definir o nível de segurança baixo quando estiver a trabalhar com aplicações que consomem muitos recursos.

Antes de activar o nível de segurança baixo, recomendamos que execute a verificação completa do computador com o nível de segurança elevado.

Se nenhum dos níveis predefinidos responder às suas necessidades, você pode configurar por si só as definições (ver secção "Protecção do sistema de ficheiros do computador" na página 42) do Antivírus de Ficheiros. Como resultado, o nome do nível de segurança alterar-se-á para **Configurações Personalizadas**. Para restaurar as predefinições da componente, seleccione um dos níveis de segurança predefinidos.

Para alterar o actual nível de segurança dos ficheiros e da memória, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Defina o nível de segurança desejado para a componente que seleccionou.

ALTERAR AS ACÇÕES A EXECUTAR COM OBJECTOS DETECTADOS

Como resultado da verificação, o Antivírus de Ficheiros atribui um dos seguintes estados aos objectos detectados:

- programa malicioso (tais como, um *vírus* ou um *Trojan*);
- estado de *potencialmente infectado* quando a verificação não consegue determinar se o objecto está infectado. Isto significa que a aplicação detectou no ficheiro uma secção de código de um vírus desconhecido ou código alterado de um vírus conhecido.

Se o Kaspersky Anti-Virus detectar objectos infectados ou potencialmente infectados durante uma verificação de vírus, você será notificado sobre isso. Deve reagir à ameaça, seleccionando uma acção a executar com o objecto. O Kaspersky Anti-Virus selecciona a opção **Perguntar o que fazer** como a acção a executar com um objecto detectado, a qual é a configuração predefinida. Você pode alterar a acção. Por exemplo, você tem a certeza de que deveria tentar desinfectar cada objecto detectado e não deseja seleccionar a acção **Desinfectar** sempre que recebe uma notificação sobre a detecção de um objecto infectado ou suspeito. Neste caso, deve seleccionar a seguinte acção: **Não perguntar o que fazer. Desinfectar**.

Antes de tentar desinfectar ou apagar um objecto infectado, o Kaspersky Anti-Virus cria uma cópia de segurança do mesmo para permitir o seu restauro ou desinfecção posterior.

Se estiver a trabalhar em modo automático (ver secção "Passo 2. Seleccionar um modo de protecção" na página 28), o Kaspersky Anti-Virus aplicará automaticamente a acção recomendada pelos especialistas da Kaspersky Lab quando forem detectados objectos perigosos. Para objectos maliciosos a acção será **Desinfectar. Apagar se não for possível desinfectar**, enquanto para objectos suspeitos a acção é – **Ignorar**.

Para alterar a acção especificada a executar com objectos detectados:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Especifique a acção desejada para a componente que seleccionou.

CRIAR UM ÂMBITO DE PROTECÇÃO

Um âmbito de protecção deve ser entendido não só como o local dos objectos a verificar, mas também o tipo de ficheiros a verificar. Por defeito, o Kaspersky Anti-Virus apenas verifica ficheiros potencialmente infectáveis iniciados a partir de qualquer disco rígido, unidade de rede ou meios amovíveis.

Você pode alargar ou reduzir o âmbito de protecção, adicionando / removendo objectos a verificar, ou alterando o tipo de ficheiros a verificar. Por exemplo, você deseja verificar apenas ficheiros *exe* executados a partir das unidades de rede. Contudo, deve certificar-se de que quando reduz o âmbito de protecção, não está a expor o seu computador à ameaça de infecção.

Ao seleccionar os tipos de ficheiro, deve lembrar-se do seguinte:

- Existem alguns formatos de ficheiros (por exemplo, *txt*) que têm um risco reduzido de possuírem código malicioso que possa ser, subsequentemente, activado. Por outro lado, existem formatos de ficheiros que contém ou podem conter código executável (*.exe*, *.dll*, *.doc)*. O risco de activação do código malicioso nesses ficheiros é bastante elevado.
- O intruso pode enviar um vírus para o seu computador com a extensão *txt*, que pode na realidade ser um ficheiro executável renomeado como um ficheiro *txt*. Se seleccionou a opção **Ficheiros verificados por extensão**, a verificação ignoraria tal ficheiro. Se a configuração **Ficheiros verificados por formato** foi seleccionada, então o Antivírus de Ficheiros irá analisar o cabeçalho do ficheiro, independentemente da extensão, detectará que o ficheiro é um ficheiro *.exe* e verificá-lo-á quanto à presença de vírus.

Para editar a lista de objectos verificados:

1. Abra a janela principal da aplicação e clique na ligação **Configuração**.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela que se abre, no separador **Geral**, na secção **Âmbito de Protecção**, clique na ligação **Adicionar**.
5. Na janela **Seleccionar objecto a verificar**, seleccione um objecto e clique no botão **Adicionar**.
6. Depois de ter adicionado todos os objectos desejados, clique no botão **OK** na janela **Seleccionar objecto a verificar**.
7. Para excluir quaisquer objectos da lista de objectos a verificar, desmarque as caixas junto aos mesmos.

Para alterar o tipo de objectos a verificar:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Seleccione a configuração desejada na janela que se abre, no separador **Geral**, na secção **Tipos de ficheiros**.

UTILIZAR A ANÁLISE HEURÍSTICA

Os objectos são verificados utilizando bases de dados que contêm descrições de todos os programas maliciosos conhecidos e dos respectivos métodos de desinfecção. O Kaspersky Anti-Virus compara cada objecto verificado com os registos da base de dados para determinar com certeza se o objecto é malicioso e, caso seja, em que classe de programa malicioso se enquadra. Esta abordagem é denominada de *análise de assinaturas* e, por defeito, é sempre utilizada.

Uma vez que surgem diariamente novos objectos maliciosos, existe sempre software malicioso que não está descrito nas bases de dados e que só pode ser detectado através da análise heurística. Este método assume a análise das acções executadas por um objecto no sistema. Se essas acções forem típicas de objectos maliciosos, é provável que o objecto seja classificado como malicioso ou suspeito. Isto permite que as novas ameaças sejam detectadas, mesmo antes de serem investigadas pelos analistas de vírus.

Se for detectado um objecto malicioso, você receberá uma notificação a solicitar a acção a aplicar.

Adicionalmente, você pode definir o nível de detalhe para as verificações. Este nível define o equilíbrio entre a minúcia das verificações de novas ameaças, a carga sobre os recursos do sistema operativo e o tempo necessário para a verificação. Quanto mais elevado for o nível de detalhe, maior a quantidade de recursos de sistema que a verificação irá requerer e maior a duração da verificação.

Para utilizar a análise heurística e definir o nível de detalhe para verificações:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela que se abre, no separador **Desempenho**, na secção **Métodos de verificação**, assinale a caixa **Análise heurística** e especifique o nível de detalhe para a verificação.

OPTIMIZAÇÃO DA VERIFICAÇÃO

Para reduzir a duração das verificações e para aumentar a velocidade de funcionamento do Kaspersky Anti-Virus, você pode optar por verificar apenas os ficheiros novos e ficheiros que foram alterados desde a última análise. Este modo aplica-se aos ficheiros simples e compostos.

- *Para verificar apenas os ficheiros novos e os ficheiros que foram alterados desde a sua última verificação:*

    1. Abra a janela principal da aplicação e clique na ligação **Configuração**.
    2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
    3. Clique no botão **Configuração** para a componente que seleccionou.
    4. Na janela que se abre, no separador **Desempenho**, na secção **Optimização da verificação**, assinale a caixa **Verificar apenas os ficheiros novos e modificados**.

VERIFICAÇÃO DE FICHEIROS COMPOSTOS

Um método comum de ocultar vírus é incorporá-los em ficheiros compostos: arquivos, bases de dados, etc. Para detectar vírus que estão ocultos dessa forma, tem de se descompactar um ficheiro composto, o que pode reduzir significativamente a velocidade da verificação.

Os pacotes de instalação e ficheiros que contêm objectos OLE são executados quando são abertos, tornando-os mais perigosos do que os arquivos. Ao desactivar a verificação de arquivos e activar a verificação deste tipo de ficheiros, você protege o seu computador contra a execução de código malicioso e, ao mesmo tempo, aumenta a velocidade de verificação.

Por defeito, o Kaspersky Anti-Virus apenas verifica objectos OLE incorporados.

- *Para alterar a lista de ficheiros compostos verificados:*

    1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
    2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
    3. Clique no botão **Configuração** para a componente que seleccionou.
    4. Na janela que se abre, no separador **Desempenho**, na secção **Verificação de ficheiros compostos**, assinale as caixas dos tipos de ficheiros compostos a serem verificados pela aplicação.

VERIFICAR FICHEIROS COMPOSTOS EXTENSOS

Quando os ficheiros compostos extensos são verificados, a sua descompactação preliminar pode demorar muito tempo. Este tempo pode ser reduzido se os ficheiros forem verificados em 2.º plano. Se for detectado um objecto malicioso enquanto trabalha com esse ficheiro, a aplicação irá notificá-lo sobre isso.

Para encurtar o tempo de espera no acesso aos ficheiros compostos, pode-se desactivar a descompactação dos ficheiros que tenham um tamanho superior ao valor especificado. Quando os ficheiros são extraídos de um arquivo, estes serão sempre verificados.

- *Para que o Kaspersky Anti-Virus faça a descompactação dos ficheiros extensos em 2.º plano, execute as seguintes acções:*

    1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
    2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
    3. Clique no botão **Configuração** para a componente que seleccionou.
    4. Na janela que se abre, no separador **Desempenho**, na secção **Verificação de ficheiros compostos**, clique no botão **Adicional**.
    5. Na janela **Ficheiros Compostos**, assinale a caixa **Extrair ficheiros compostos em 2.º plano** e especifique o tamanho mínimo do ficheiro no campo por baixo.

- *Para que o Kaspersky Anti-Virus não descompacte os ficheiros compostos extensos, execute as seguintes acções:*

    1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
    2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
    3. Clique no botão **Configuração** para a componente que seleccionou.
    4. Na janela que se abre, no separador **Desempenho**, na secção **Verificação de ficheiros compostos**, clique no botão **Adicional**.
    5. Na janela **Ficheiros compostos** que se abre, assinale a caixa **Não descompactar ficheiros compostos extensos** e especifique o tamanho do ficheiro no campo ao lado.

ALTERAR O MODO DE VERIFICAÇÃO

O modo de verificação é a condição que acciona a actividade do Antivírus de Ficheiros. Por defeito, o Kaspersky Anti-Virus utiliza o modo inteligente, o qual determina se o objecto está sujeito a verificação com base nas acções executadas com o mesmo. Por exemplo, quando trabalhar com um documento do Microsoft Office, o Kaspersky Anti-Virus verifica o ficheiro, primeiro, quando este é aberto e, por último, quando este é fechado. As operações intermédias gravadas no ficheiro não fazem com que o mesmo seja verificado.

Pode alterar o modo de verificação de objectos. O modo de verificação deve ser seleccionado dependendo dos ficheiros com os quais trabalha mais frequentemente.

- *Para alterar o modo de verificação de objectos:*

    1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
    2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
    3. Clique no botão **Configuração** para a componente que seleccionou.
    4. Na janela que se abre, no separador **Adicional**, na secção **Modo de verificação**, seleccione o modo desejado.

TECNOLOGIA DE VERIFICAÇÃO

Também pode especificar as tecnologias que serão utilizadas pela componente Antivírus de Ficheiros:

- **iChecker**. Esta tecnologia pode aumentar a velocidade de verificação, excluindo determinados objectos da verificação. Um objecto é excluído da verificação, utilizando um algoritmo especial que toma em consideração a data de distribuição das bases de dados do Kaspersky Anti-Virus, a data em que o objecto foi verificado pela última vez e quaisquer alterações às definições de verificação.

  Por exemplo, você tem um arquivo ao qual foi atribuído o estado *não infectado* após a verificação. Na próxima vez, a aplicação irá excluir este arquivo da verificação, excepto se tiver sido alterado ou se as definições de verificação tiverem sido alteradas. Se a estrutura do arquivo tiver sido alterada devido a um novo objecto adicionado ao mesmo, se as definições de verificação tiverem sido alteradas ou se as bases de dados da aplicação tiverem sido actualizadas, a aplicação irá verificar novamente o arquivo.

  Existem limitações no iChecker: não funciona com ficheiros extensos e apenas se aplica a objectos com uma estrutura que a aplicação reconheça (por exemplo *.exe*, *.dll*, *.lnk*, *.ttf*, *.inf*, *.sys*, *.com*, *.chm*, *.zip*, *.rar*).

- **iSwift**. Esta tecnologia é um desenvolvimento da tecnologia iChecker para computadores que usam sistemas de ficheiros NTFS. Existem limitações no iSwift: está limitada a um local específico no sistema de ficheiros e só pode ser aplicada a objectos num sistema de ficheiros NTFS.

Para alterar a tecnologia de verificação de objectos:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela que se abre, no separador **Adicional**, na secção **Tecnologias de verificação**, seleccione o modo desejado.

PAUSAR A COMPONENTE: CRIAR UM AGENDAMENTO

Quando estão em execução determinados programas que requerem recursos significativos do computador, você pode pausar temporariamente o funcionamento da componente Antivírus de Ficheiros, o que permite um acesso mais rápido aos objectos. Para reduzir a carga sobre o computador e assegurar o acesso rápido aos objectos, você pode definir um agendamento para a desactivação da componente.

Figura 7. Criar um agendamento

Para configurar um agendamento para pausar a componente:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela que se abre, no separador **Adicional**, na secção **Pausar tarefa**, assinale a caixa **Planificadas** e clique no botão **Agendamento**.
5. Na janela **Pausar a tarefa**, especifique a hora (no formato de 24 horas HH:MM) durante o qual a protecção será pausada (campos **Pausar tarefa às** e **Continuar tarefa às**).

PAUSAR A COMPONENTE: CRIAR UMA LISTA DE APLICAÇÕES

Quando estão em execução determinados programas que requerem recursos significativos do computador, você pode pausar temporariamente o funcionamento da componente Antivírus de Ficheiros, o que permite um acesso mais rápido aos objectos. Para reduzir a carga sobre o computador e assegurar o acesso rápido aos objectos, você pode configurar as definições para a desactivação da componente quando trabalhar com determinadas aplicações.

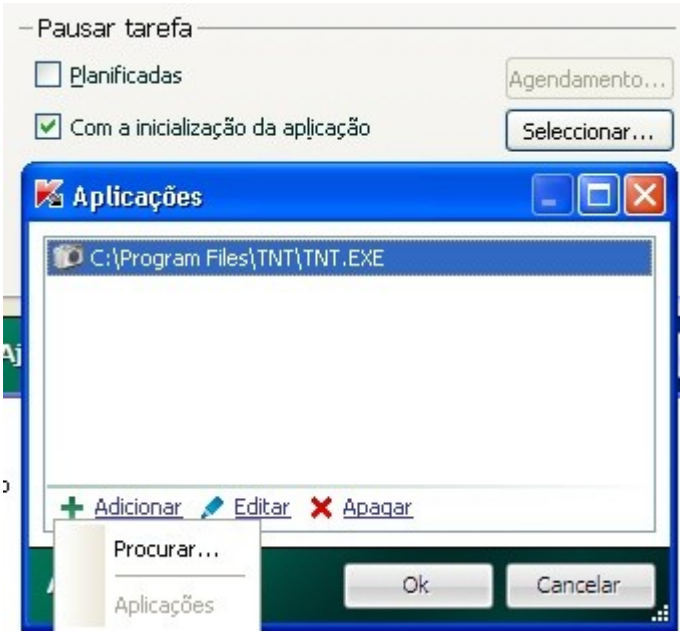


Figura 8. Criar uma lista de aplicações

A configuração da desactivação do Antivírus de Ficheiros em caso de conflito com determinadas aplicações é uma medida drástica. Se ocorrerem conflitos ao trabalhar com a componente, por favor contacte o Suporte Técnico da Kaspersky Lab (http://support.kaspersky.pt). Os especialistas de suporte podem ajudá-lo a resolver os problemas de funcionamento simultâneo do Kaspersky Anti-Virus com o software do seu computador.

Para configurar a pausa da componente quando determinadas aplicações estiverem a ser usadas, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela que se abre, no separador **Adicional**, na secção **Pausar tarefa**, assinale a caixa **Com a inicialização da aplicação** e clique no botão **Seleccionar**.
5. Na janela **Aplicações**, crie uma lista de aplicações cuja inicialização irá pausar o funcionamento da componente.

RESTAURAR AS PREDEFINIÇÕES DE PROTECÇÃO

Ao configurar o Antivírus de Ficheiros, pode sempre restaurar as respectivas definições recomendadas. Estas são consideradas óptimas, recomendadas pela Kaspersky Lab e agrupadas no nível de segurança **Recomendado**.

Para restaurar as predefinições de protecção, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Na secção **Nível de Segurança**, clique no botão **Nível predefinido** para a componente seleccionada.

PROTECÇÃO DE E-MAILS

O *Antivírus de E-mail* verifica os e-mails de entrada e de saída quanto à presença de objectos maliciosos. Este é iniciado quando o sistema operativo é carregado, está localizado na memória RAM do computador e verifica todos os e-mails recebidos através dos protocolos POP3, SMTP, IMAP, MAPI e NNTP.

A forma como os e-mails são verificados é determinada por um conjunto de definições denominado de nível de segurança. Se for detectada uma ameaça, o Antivírus de E-mail irá executar a acção que especificou (ver secção "Alterar as acções a executar com objectos detectados" na página 54). As regras, com as quais os seus e-mails são verificados, são determinadas por um conjunto de definições. Estas podem ser divididas em grupos, que determinam as seguintes características:

- do fluxo protegido de e-mails;
- da utilização de métodos de análise heurística;
- da verificação de ficheiros compostos;
- da filtragem de ficheiros anexados.

A Kaspersky Lab recomenda que não configure sozinho o Antivírus de E-mail. Na maioria dos casos, será suficiente seleccionar um nível de segurança diferente. Pode restaurar as predefinições do Antivírus de E-mail. Para o fazer, seleccione um dos níveis de segurança.

Para editar a configuração do Antivírus de E-mail, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Faça as alterações necessárias na configuração da componente.

NESTA SECÇÃO:

Algoritmo de funcionamento da componente 53

Alterar o nível de segurança da protecção de e-mail 54

Alterar as acções a executar com objectos detectados..... 54

Criar um âmbito de protecção 55

Verificar e-mails no Microsoft Office Outlook..... 56

Verificar e-mails no The Bat! 56

Utilizar a Análise Heurística..... 57

Verificação de ficheiros compostos 57

Filtrar anexos..... 58

Restaurar as predefinições da protecção de e-mail 58

ALGORITMO DE FUNCIONAMENTO DA COMPONENTE

O Kaspersky Anti-Virus inclui a componente *Antivírus de E-mail*, que garante a verificação dos e-mails em relação a objectos perigosos. Este é carregado quando o sistema operativo é iniciado e está sempre em execução, verificando todos os e-mails com os protocolos POP3, SMTP, IMAP, MAPI e NNTP, assim como ligações seguras (SSL) para POP3 e IMAP.

O indicador de funcionamento da componente é o ícone da aplicação na área de notificação da barra de tarefas, que apresenta este aspecto sempre que um e-mail está a ser verificado.

Por defeito, a protecção de e-mails é efectuada da seguinte forma:

1. Cada e-mail recebido ou enviado pelo utilizador é interceptado pela componente.

2. O e-mail é decomposto nas suas partes: o cabeçalho do e-mail, o seu corpo e os anexos.

3. O corpo e os anexos do e-mail (incluindo objectos OLE) são verificados quanto à existência de objectos perigosos. Os objectos maliciosos são detectados com as bases de dados utilizadas pelo Kaspersky Anti-Virus e com um algoritmo heurístico. A base de dados contém descrições de todos os programas maliciosos conhecidos até à data e dos métodos para os neutralizar. O algoritmo heurístico consegue detectar novos vírus que ainda não foram inseridos na base de dados.

4. Depois da verificação de vírus, estão disponíveis as seguintes opções de comportamento:

   - Se o corpo ou os anexos do e-mail contiverem código malicioso, a componente Antivírus de E-mail bloqueará o e-mail, criará uma cópia de segurança do mesmo e tentará desinfectar o objecto. Depois de o e-mail ser desinfectado com sucesso, o mesmo é devolvido ao utilizador. Se a desinfecção falhar, o objecto infectado será apagado da mensagem. Depois da verificação de vírus, é inserido um texto especial na linha de assunto do e-mail, referindo que o e-mail foi processado pelo Kaspersky Anti-Virus.

   - Se no corpo ou nos anexos for detectado código potencialmente malicioso (mas não houver certeza absoluta de que é malicioso), a parte suspeita do e-mail será colocada numa área de armazenamento especial, denominada Quarentena.

   - Se não for detectado qualquer código malicioso no e-mail, o mesmo é imediatamente disponibilizado ao utilizador.

É fornecido um módulo de extensão integrado para o Microsoft Office Outlook (ver secção "Verificar e-mails no Microsoft Office Outlook" na página 56) que permite ajustar o cliente de e-mail.

Se está a utilizar o The Bat!, o Kaspersky Anti-Virus pode ser utilizado em conjunto com outras aplicações de antivírus. As regras de processamento do tráfego de e-mail (ver secção "Verificar e-mails no The Bat!" na página 56) são configuradas directamente no The Bat! e substituem as definições de protecção de e-mail da aplicação.

Ao trabalhar com outros programas de e-mail, incluindo o Microsoft Outlook Express/Programa de E-mail do Windows, Mozilla Thunderbird, Eudora, e Incredimail, a componente Antivírus de E-mail verifica e-mails com os protocolos SMTP, POP3, IMAP e NNTP.

Note que ao trabalhar com o cliente de e-mail Thunderbird, os e-mails transmitidos através do protocolo IMAP não serão verificados quanto à presença de vírus, se estiver utilizar filtros que os movem para fora da pasta **Caixa de Entrada**.

ALTERAR O NÍVEL DE SEGURANÇA DA PROTECÇÃO DE E-MAIL

O nível de segurança é uma configuração predefinida do Antivírus de E-mail. Os especialistas da Kaspersky Lab distinguem três níveis de segurança. A decisão sobre o nível de segurança a seleccionar tem de ser tomada pelo utilizador, com base nas condições de funcionamento e na situação actual. Pode seleccionar um dos seguintes níveis de segurança:

- **Elevado**. Se trabalha num ambiente inseguro, o nível de segurança máximo será o mais adequado para si. Um exemplo de um ambiente desse tipo é a ligação a um serviço de e-mail gratuito, a partir de uma rede que não está guardada por uma protecção de e-mail centralizada.

- **Recomendado**. Este nível fornece um equilíbrio entre eficiência e segurança e é adequado para a maioria dos casos. Este é também a configuração predefinida.

- **Baixo**. Se trabalha num ambiente bem protegido, pode utilizar o nível de segurança baixo. Um exemplo de um ambiente desse tipo pode ser uma rede empresarial com segurança de e-mail centralizada.

Se nenhum dos níveis predefinidos responder às suas necessidades, você pode configurar por si só as definições (ver secção "Protecção de E-mails" na página 52) do Antivírus de E-mail. Como resultado, o nome do nível de segurança alterar-se-á para **Configurações Personalizadas**. Para restaurar as predefinições da componente, seleccione um dos níveis de segurança predefinidos.

Para alterar o nível de segurança de e-mail predefinido:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.

2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.

3. Defina o nível de segurança desejado para a componente que seleccionou.

ALTERAR AS ACÇÕES A EXECUTAR COM OBJECTOS DETECTADOS

O Antivírus de E-mail verifica um e-mail. Se a verificação indicar que o e-mail ou qualquer uma das suas partes (corpo, anexo) está infectado ou potencialmente infectado, as acções adicionais da componente dependem do estado do objecto e da acção seleccionada.

Como resultado da verificação, o Antivírus de E-mail atribui um dos seguintes estados aos objectos detectados:

- programa malicioso (tais como, um *vírus* ou um *Trojan*).

- estado de *potencialmente infectado* quando a verificação não consegue determinar se o objecto está infectado. Isto significa que o e-mail ou anexo contém uma sequência de código de um vírus desconhecido ou código alterado de um vírus conhecido.

Se o Kaspersky Anti-Virus detectar objectos infectados ou potencialmente infectados durante uma verificação de e-mail, você será notificado sobre isso. Deve reagir à ameaça, seleccionando uma acção a executar com o objecto. O Kaspersky Anti-Virus selecciona a opção **Perguntar o que fazer** como a acção a executar com um objecto detectado, a qual é a configuração predefinida. Você pode alterar a acção. Por exemplo, você tem a certeza de que deveria tentar desinfectar cada objecto detectado e não deseja seleccionar a acção **Desinfectar** sempre que recebe uma notificação sobre a detecção de um outro objecto infectado ou suspeito num e-mail. Neste caso, deve seleccionar a seguinte acção: **Não perguntar o que fazer. Desinfectar**.

Antes de tentar desinfectar ou apagar um objecto infectado, o Kaspersky Anti-Virus cria uma cópia de segurança do mesmo para permitir o seu restauro ou desinfecção posterior.

Se estiver a trabalhar em modo automático (ver secção "Passo 2. Seleccionar um modo de protecção" na página 28), o Kaspersky Anti-Virus aplicará automaticamente a acção recomendada pelos especialistas da Kaspersky Lab quando forem detectados objectos perigosos. Para objectos maliciosos a acção será **Desinfectar. Apagar se não for possível desinfectar**, enquanto para objectos suspeitos a acção é – **Ignorar**.

- *Para alterar a acção especificada a executar com objectos detectados:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
  3. Especifique a acção desejada para a componente que seleccionou.

CRIAR UM ÂMBITO DE PROTECÇÃO

O âmbito de protecção é entendido como o tipo de mensagens a verificar. Por defeito, o Kaspersky Anti-Virus verifica quer os e-mails de entrada, quer os e-mails de saída. Se tiver escolhido verificar apenas os e-mails de entrada, recomenda-se que verifique os e-mails de saída quando começar a utilizar o Kaspersky Anti-Virus uma vez que é provável que existam worms no seu computador que se distribuem através do e-mail. Isto ajudará a evitar situações indesejáveis causadas pelo envio em massa e não monitorizado de e-mails infectados a partir do seu computador.

O âmbito de protecção também inclui as configurações utilizadas para integrar a componente Antivírus de E-mail no sistema e os protocolos a verificar. Por defeito, a componente Antivírus de E-mail está integrada nos clientes de e-mail Microsoft Office Outlook e The Bat!.

- *Para desactivar as verificações dos e-mails enviados, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
  3. Clique no botão **Configuração** para a componente que seleccionou.
  4. Na janela que se abre, no separador **Geral**, na secção **Âmbito de Protecção**, especifique os valores desejados para as definições.

- *Para seleccionar os protocolos a verificar e as definições para integrar o Antivírus de E-mail no sistema, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
  3. Clique no botão **Configuração** para a componente que seleccionou.
  4. Na janela que se abre, no separador **Adicional**, na secção **Conectividade**, seleccione as configurações desejadas.

VERIFICAR E-MAILS NO MICROSOFT OFFICE OUTLOOK

Se utiliza o Microsoft Office Outlook como o seu cliente de e-mail, pode configurar definições adicionais para verificar a existência de vírus nos seus e-mails.

Quando instala o Kaspersky Anti-Virus, é instalado um plug-in (extensão) especial no Microsoft Office Outlook. Esta extensão permite-lhe configurar rapidamente as definições do Antivírus de E-mail e ainda determinar em que altura os e-mails serão verificados quanto à existência de objectos perigosos.

O plug-in aparece sob a forma de um separador especial **Protecção de e-mail**, que está localizado no menu **Ferramentas** → **Opções**. No separador pode especificar os modos de verificação de e-mail.

Para especificar as condições de filtragem complexa:

1. Abra a janela principal do Microsoft Office Outlook.
2. Seleccione **Ferramentas** → **Opções** a partir do menu da aplicação.
3. No separador **Protecção de e-mail** especifique o modo de verificação de e-mail desejado.

VERIFICAÇÃO DE E-MAILS NO THE BAT!

No programa The Bat!, as acções executadas sobre objectos de e-mail infectados são definidas com as ferramentas da própria aplicação.

As definições do Antivírus de E-mail, que determinam se os e-mails de entrada ou de saída são verificados, que determinam as acções executadas sobre objectos de e-mail perigosos e as exclusões aplicadas, são ignoradas. As únicas definições que o The Bat! toma em consideração é a verificação de arquivos anexados.

As definições de protecção de e-mail aplicam-se a todos os módulos antivírus instalados no computador e que apoiam o trabalho efectuado com o The Bat!.

Por favor, lembre-se que quando são recebidos e-mails, primeiro estes são verificados pelo Antivírus de E-mail e só depois pela extensão do The Bat!. Quando é detectado um objecto malicioso, o Kaspersky Anti-Virus irá informá-lo sobre isso. Se seleccionar a acção **Desinfectar** (**Apagar**) na janela de notificação do Antivírus de E-mail, as acções destinadas a eliminar a ameaça serão executadas pelo Antivírus de E-mail. Se seleccionar a acção **Ignorar** na janela de notificação, o objecto será desinfectado pela extensão do The Bat!. Ao enviar e-mails, primeiro a verificação é efectuada pela extensão e depois pelo Antivírus de E-mail.

Tem que decidir:

- Que fluxo de e-mails será verificado (e-mails de entrada, e-mails de saída).
- em que altura os objectos de e-mail serão verificados, quanto à existência de vírus (quando abrir um e-mail ou antes de guardar um e-mail no disco);
- As acções que serão executadas pelo cliente de e-mail quando são detectados objectos perigosos em e-mails. Por exemplo, pode seleccionar:
  - **Tentar desinfectar partes infectadas** – se esta opção for seleccionada, tentar-se-á desinfectar o objecto infectado; se o mesmo não puder ser desinfectado, o objecto permanecerá no e-mail.
  - **Apagar partes infectadas** – se esta opção for seleccionada, o objecto de e-mail perigoso será apagado, independentemente de o objecto estar infectado ou se suspeitar de estar infectado.

Por defeito, o The Bat! coloca na Quarentena todos os objectos de e-mail infectados, sem tentar desinfectá-los.

O The Bat! não atribui cabeçalhos especiais para os e-mails que contêm objectos perigosos.

Para configurar as regras de protecção de e-mail no The Bat!:

1. Abra a janela principal do The Bat!.
2. Seleccione o item **Definições** no menu **Propriedades** do cliente de e-mail.
3. Seleccione o item **Protecção de vírus** na árvore de configurações.

UTILIZAR A ANÁLISE HEURÍSTICA

Em termos básicos, o método heurístico analisa as actividades do objecto no sistema. Se essas acções forem típicas de objectos maliciosos, é provável que o objecto seja classificado como malicioso ou suspeito. Isto permite que as novas ameaças sejam detectadas, mesmo antes de serem analisadas pelos analistas de vírus. Por defeito, a análise heurística está activada.

O Kaspersky Anti-Virus irá notificá-lo quando for detectado um objecto malicioso numa mensagem. Você deve reagir às notificações, continuando com o processamento da mensagem.

Adicionalmente, você pode definir o nível de detalhe para as verificações: **nível superficial**, **nível médio**, ou **nível aprofundado**. Para o fazer, ajuste a barra indicadora para a posição seleccionada.

Para activar/desactivar a análise heurística e para definir o nível de detalhe para a verificação, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela que se abre, no separador **Geral**, na secção **Métodos de verificação**, assinale / desmarque a caixa **Análise heurística** e especifique o nível de detalhe para a verificação.

VERIFICAÇÃO DE FICHEIROS COMPOSTOS

A selecção do modo de verificação de ficheiros compostos afecta o desempenho do Kaspersky Anti-Virus. Você pode activar ou desactivar a verificação dos arquivos anexados e limitar o tamanho máximo dos arquivos a verificar.

Para configurar as definições da verificação de ficheiros compostos:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela que se abre, no separador **Geral**, seleccione o modo de verificação de ficheiros compostos.

FILTRAR ANEXOS

Pode configurar as condições de filtragem para os anexos de e-mail. Ao utilizar o filtro, pode melhorar a segurança do seu computador, uma vez que os programas maliciosos espalham-se através de e-mails e, mais frequentemente, são enviados como anexos. Ao renomear ou apagar determinados tipos de anexos, você pode proteger o seu computador contra perigos potenciais, como por exemplo a abertura automática de anexos quando é recebida uma mensagem.

Se o seu computador não está protegido por nenhum software de rede local (você acede directamente à Internet, sem nenhum servidor de proxy ou firewall), recomenda-se que não desactive a verificação de arquivos anexados.

Para configurar as definições da filtragem de anexos:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela que se abre, no separador **Filtro de anexos**, especifique as condições de filtragem de anexos de e-mail. Quando selecciona um destes dois últimos modos, é activada a lista de tipos de ficheiros, na qual pode especificar os tipos desejados ou adicionar uma máscara para um novo tipo.

   Se for necessário adicionar uma máscara para um novo tipo, clique na ligação **Adicionar** e insira os dados necessários na janela **Máscara de nome do ficheiro de input** que se abre.

RESTAURAR AS PREDEFINIÇÕES DA PROTECÇÃO DE E-MAIL

Ao configurar o Antivírus de E-mail, pode sempre restaurar as respectivas definições recomendadas. Estas são consideradas óptimas, recomendadas pela Kaspersky Lab e agrupadas no nível de segurança **Recomendado**.

Para restaurar as predefinições da protecção de e-mail, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
3. Na secção **Nível de Segurança**, clique no botão **Nível predefinido** para a componente seleccionada.

PROTECÇÃO DO TRÁFEGO DE INTERNET

Sempre que utiliza a Internet, você está a submeter a informação armazenada no seu computador ao risco de infecção por programas perigosos. Estes programas podem infiltrar-se no seu computador quando transfere um software grátis ou quando navega em sites que antes eram seguros e que sofreram ataques de hackers recentemente. Para além disso, os worms de rede podem penetrar no seu computador antes de você abrir uma página de Internet e transferir um ficheiro, simplesmente porque o seu computador está ligado à Internet.

A componente *Antivírus de Internet* foi concebida para garantir a segurança enquanto utiliza a Internet. Esta protege o seu computador em relação aos dados que entram no computador através do protocolo HTTP e também impede que sejam executados scripts perigosos no computador.

A protecção de Internet apenas monitoriza o tráfego de HTTP que passa através das portas incluídas na lista de portas monitorizadas. No pacote de instalação do Kaspersky Anti-Virus está incluída uma lista das portas que são mais frequentemente utilizadas para transmitir tráfego de e-mails e de HTTP. Se utiliza portas que não estão nesta lista, adicione-as à lista para proteger o tráfego efectuado através dessas portas.

Se está a trabalhar num espaço desprotegido, recomenda-se que utilize o Antivírus de Internet enquanto trabalha na Internet. Se o seu computador está a funcionar numa rede protegida por uma firewall ou filtros de tráfego de HTTP, o Antivírus de Internet fornece-lhe segurança adicional na utilização da Internet.

Um conjunto de definições, denominado de nível de segurança, determina a forma de verificação do tráfego. Se o Antivírus de Internet detectar uma ameaça, este irá executar a acção definida.

O seu nível de protecção da Internet é determinado por um grupo de definições. As definições podem ser decompostas nos seguintes grupos:

- definições relacionadas com o âmbito de protecção;
- definições que determinam a eficiência da protecção do tráfego (utilização da análise heurística, optimização da verificação).

A Kaspersky Lab recomenda que não configure sozinho a componente Antivírus de Internet. Na maioria dos casos, será suficiente seleccionar um nível de segurança diferente.

➡ *Para editar a configuração do Antivírus de Internet:*

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Faça as alterações necessárias na configuração da componente.

NESTA SECÇÃO:

Algoritmo de funcionamento da componente 60

Alterar o nível de segurança do tráfego de HTTP 61

Alterar as acções a executar com objectos detectados 61

Criar um âmbito de protecção 62

Seleccionar o tipo de verificação 62

Conselheiro de URLs da Kaspersky 63

Utilizar a Análise Heurística 64

Optimização da verificação 64

Restaurar as predefinições de protecção da Internet 65

ALGORITMO DE FUNCIONAMENTO DA COMPONENTE

O *Antivírus de Internet* protege o seu computador em relação aos dados que entram no computador através do protocolo HTTP e também impede que sejam executados scripts perigosos no computador.

Esta secção aborda o funcionamento da componente com maior detalhe. O tráfego de HTTP é protegido através do seguinte algoritmo:

1. Cada página de Internet ou ficheiro acedido pelo utilizador ou por um determinado programa, através do protocolo HTTP, é interceptado e analisado pelo Antivírus de Internet, quanto à existência de código malicioso. Os objectos maliciosos são detectados, utilizando as bases de dados do Kaspersky Anti-Virus e o algoritmo heurístico. A base de dados contém descrições de todos os programas maliciosos conhecidos até à data e dos métodos para os neutralizar. O algoritmo heurístico consegue detectar novos vírus que ainda não foram inseridos na base de dados.

2. Após a análise, você tem à disposição as seguintes acções:

   - Se a página de Internet ou objecto acedido pelo utilizador contiverem código malicioso, o acesso aos mesmos é bloqueado. Depois, surge uma notificação, referindo que a página ou o objecto solicitado estão infectados.

   - Se o ficheiro ou a página de Internet não contiverem código malicioso, estes são imediatamente disponibilizados ao utilizador pelo programa.

Os scripts são verificados de acordo com o seguinte algoritmo:

1. Cada script, executado numa página de Internet, é interceptado pelo Antivírus de Internet e é analisado quanto à presença de código malicioso.

2. Se o script contiver código malicioso, o Antivírus de Internet bloqueia-o e informa o utilizador através de uma mensagem especial que surge no ecrã.

3. Se não for detectado qualquer código malicioso no script, o mesmo é executado.

Os scripts apenas são interceptados nas páginas de Internet abertas no Microsoft Internet Explorer.

ALTERAR O NÍVEL DE SEGURANÇA DO TRÁFEGO DE HTTP

O nível de segurança é uma configuração predefinida do Antivírus de E-mail. Os especialistas da Kaspersky Lab distinguem três níveis de segurança. A decisão sobre o nível de segurança a seleccionar tem de ser tomada pelo utilizador, com base nas condições de funcionamento e na situação actual. Terá a possibilidade de seleccionar uma das seguinte opções para o nível de segurança:

- **Elevado**. Este nível de segurança é recomendado para ambientes sensíveis, quando não estão a ser utilizadas outras ferramentas de segurança de HTTP.
- **Recomendado**. Este nível de segurança é óptimo para utilizar na maioria dos casos.
- **Baixo**. Use este nível de segurança se tiver instalado no seu computador ferramentas adicionais de protecção do tráfego de HTTP.

Se nenhum dos níveis predefinidos responder às suas necessidades, você pode configurar por si só as definições (ver secção "Protecção do tráfego de Internet" na página 59) do Antivírus de Internet. Como resultado, o nome do nível de segurança alterar-se-á para **Configurações Personalizadas**. Para restaurar as predefinições da componente, seleccione um dos níveis de segurança predefinidos.

Para alterar o nível de segurança predefinido para o tráfego de Internet:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Defina o nível de segurança desejado para a componente que seleccionou.

ALTERAR AS ACÇÕES A EXECUTAR COM OBJECTOS DETECTADOS

Quando a análise de um objecto de HTTP revelar que este contém código malicioso, a resposta da componente Antivírus de Internet depende da acção que tiver seleccionado.

O Antivírus de Internet bloqueia sempre as acções de objectos perigosos e emite mensagens de pop-up que informam o utilizador sobre a acção executada. Você não pode alterar a acção executada em relação a um script perigoso. A única alteração disponível é desactivar o módulo de verificação de scripts (ver secção "Seleccionar o tipo de verificação" na página 62).

Se estiver a trabalhar em modo automático (ver secção "Passo 2. Seleccionar um modo de protecção" na página 28), o Kaspersky Anti-Virus aplicará automaticamente a acção recomendada pelos especialistas da Kaspersky Lab quando forem detectados objectos perigosos.

Para alterar a acção especificada a executar com objectos detectados:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Especifique a acção desejada para a componente que seleccionou.

CERROR! BOOKMARK NOT DEFINED.RIAR UM ÂMBITO DE PROTECÇÃO

Criar um âmbito de protecção significa seleccionar o tipo de verificação (ver secção "Seleccionar o tipo de verificação" na página 62) de objectos pelo Antivírus de Internet e criar a lista de endereços confiáveis, que contém informação não sujeita a verificação pela componente, no que respeita a objectos perigosos.

Você pode criar uma lista de endereços confiáveis, em cujos conteúdos você confia incondicionalmente. O Antivírus de Internet não analisará os dados desses endereços quanto à presença de objectos perigosos. Esta opção pode ser útil nos casos em que, por exemplo, o Antivírus de Internet interfere com a transferência de um determinado ficheiro.

Para criar a lista de endereços confiáveis, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela **Antivírus de Internet** que se abre, na secção **Optimização da verificação**, assinale a caixa **Não verificar tráfego de HTTP de endereços de Internet confiáveis** e clique no botão **Seleccionar**.
5. Na janela **Lista de endereços confiáveis** que se abre, clique na ligação **Adicionar**.
6. Na janela **Máscara de endereço (URL)** que se abre, insira um endereço de Internet confiável (ou uma máscara para o endereço confiável).

SELECCIONAR O TIPO DE VERIFICAÇÃO

A tarefa de criação do âmbito de protecção (ver página 62), em conjunto com a criação da lista de endereços confiáveis, também inclui a selecção do tipo de verificação do tráfego efectuada pelo Antivírus de Internet. Segundo o tipo, a verificação divide-se em verificação de scripts e verificação do tráfego de HTTP.

Por defeito, o Antivírus de Internet verifica o tráfego de HTTP e os scripts em simultâneo.

A verificação do tráfego de HTTP inclui não só a verificação de vírus, mas também a verificação de links para ver se estão presentes na lista de endereços de Internet suspeitos e/ou lista de endereços de phishing.

A verificação de links para ver se estão incluídos na lista de endereços de phishing permite evitar ataques de phishing, que, por norma, parecem mensagens de e-mail de instituições financeiras que fingem ser de boa-fé e que contêm links para os seus sites. O texto do e-mail convence o leitor a clicar no link e a inserir informações confidenciais na janela que se abre em seguida, por exemplo, um número de cartão de crédito ou um nome de utilizador e password para um site de banca online onde se podem executar operações financeiras.

Uma vez que o link para um site de phishing pode ser recebido não apenas num e-mail, mas também através de qualquer outra forma, por exemplo, no texto de uma mensagem do ICQ, o Antivírus de Internet detecta as tentativas de acesso a um site de phishing ao nível da verificação do tráfego de HTTP, e bloqueia-as.

A verificação de links para ver se estão incluídos na lista de endereços de Internet suspeitos permite controlar os sites incluídos na lista negra. A lista é criada pelos especialistas da Kaspersky Lab e está incluída no pacote de instalação da aplicação.

- *Para que o Antivírus de Internet verifique os scripts, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
  3. Clique no botão **Configuração** para a componente que seleccionou.
  4. Na janela **Antivírus de Internet** que se abre, na secção **Adicional**, certifique-se de que a caixa ☑ **Bloquear scripts perigosos no Microsoft Internet Explorer** está assinalada. O Antivírus de Internet irá verificar todos os scripts processados no Microsoft Internet Explorer, assim como quaisquer outros scripts WSH (JavaScript, Visual Basic Script, etc.) que são executados enquanto o utilizador trabalha no computador.

     Para além disso, pode utilizar o Conselheiro de URLs da Kaspersky (ver página 63). Para o fazer, assinale a caixa ☑ **Assinalar URLs de phishing e suspeitos no Microsoft Internet Explorer e Mozilla Firefox**. O Antivírus de Internet irá assinalar os URLs de phishing e suspeitos detectados em navegadores de Internet (Microsoft Internet Explorer e Mozilla Firefox).

- *Para verificar links através da base de endereços de Internet suspeitos e / ou base de endereços de phishing, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
  3. Clique no botão **Configuração** para a componente que seleccionou.
  4. Na janela **Antivírus de Internet** que se abre, na secção **Métodos de verificação**, certifique-se de que a caixa ☑ **Verificar se URLs estão listados na base de endereços de Internet suspeitos** e / ou a caixa ☑ **Verificar se URLs estão listados na base de endereços de phishing** estão assinaladas.

CONSELHEIRO DE URLS DA KASPERSKY

O Kaspersky Anti-Virus inclui o módulo de verificação de URLs gerido pelo Antivírus de Internet Este módulo verifica se os links existentes na página de Internet pertencem à lista de endereços de Internet suspeitos e de phishing. Pode criar uma lista de endereços de Internet confiáveis, cujo conteúdo não deve ser verificado, e uma lista de endereços de Internet, cujo conteúdo deve ser sempre verificado. Este módulo é integrado nos navegadores Microsoft Internet Explorer e Mozilla Firefox como uma extensão (plug-in).

- *Para activar o Conselheiro de URLs da Kaspersky, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
  3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a componente seleccionada.
  4. Na janela **Antivírus de Internet** que se abre, na secção **Adicional**, assinale a caixa ☑ **Assinalar URLs de phishing e suspeitos no Microsoft Internet Explorer e Mozilla Firefox**.

- *Para criar a lista de endereços confiáveis, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
  3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a componente seleccionada.
  4. Na janela **Antivírus de Internet** que se abre, na secção **Adicional**, clique no botão **Configuração**.
  5. Na janela **Conselheiro de URLs da Kaspersky** que se abre, seleccione a opção ◉ **Em todas as páginas de Internet** e clique no botão **Exclusões**.
  6. Na janela **Lista de endereços confiáveis** que se abre, clique na ligação **Adicionar**.
  7. Na janela **Máscara de endereço (URL)** que se abre, insira um endereço de Internet confiável (ou uma máscara para o endereço confiável).

Para criar a lista de sites cujo conteúdo deve ser verificado:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a componente seleccionada.
4. Na janela **Antivírus de Internet** que se abre, na secção **Adicional**, clique no botão **Configuração**.
5. Na janela **Conselheiro de URLs da Kaspersky** que se abre, seleccione a opção **Nas páginas de Internet seleccionadas** e clique no botão **Seleccionar**.
6. Na janela **Lista de endereços verificados** que se abre, clique na ligação **Adicionar**.
7. Na janela **Máscara de endereço (URL)** que se abre, insira o endereço de Internet (ou a sua máscara).

UTILIZAR A ANÁLISE HEURÍSTICA

Em termos básicos, o método heurístico analisa as actividades do objecto no sistema. Se essas acções forem típicas de objectos maliciosos, é provável que o objecto seja classificado como malicioso ou suspeito. Isto permite que as novas ameaças sejam detectadas, mesmo antes de serem investigadas pelos analistas de vírus. Por defeito, a análise heurística está activada.

O Kaspersky Anti-Virus irá notificá-lo quando for detectado um objecto malicioso numa mensagem. Você deve reagir às notificações, continuando com o processamento da mensagem.

Adicionalmente, você pode definir o nível de detalhe para as verificações: **nível superficial**, **nível médio**, ou **nível aprofundado**. Para o fazer, ajuste a barra indicadora para a posição seleccionada.

Para activar/desactivar a análise heurística e para definir o nível de detalhe para a verificação, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela **Antivírus de Internet** que se abre, na secção **Métodos de verificação** assinale / desmarque a caixa **Análise heurística** e por baixo especifique o nível de detalhe da verificação.

OPTIMIZAÇÃO DA VERIFICAÇÃO

Para detectar código malicioso de forma mais eficiente, o Antivírus de Internet armazena, temporariamente, os fragmentos de objectos transferidos da Internet. Ao utilizar este método, o Antivírus de Internet apenas verifica um objecto depois de este ter sido, completamente, transferido. Depois disso, o objecto é verificado em termos de vírus e, dependendo dos resultados da verificação, a aplicação devolve o objecto ao utilizador ou bloqueia-o.

Contudo, o armazenamento temporário de objectos aumenta o tempo de processamento do objecto e, desse modo, o tempo decorrido antes de a aplicação devolver os objectos ao utilizador. Isto pode causar problemas ao copiar e processar objectos extensos, uma vez que é excedido o tempo limite na ligação ao cliente de HTTP.

Para resolver este problema, sugerimos que limite o tempo de armazenamento temporário para fragmentos de objectos transferidos da Internet. Quando este tempo for excedido, o utilizador receberá a parte transferida do ficheiro sem ser verificada e quando o objecto tiver sido, integralmente, copiado, o mesmo será verificado na sua totalidade. Isso permite reduzir o tempo necessário para transferir o objecto ao utilizador e elimina o problema da interrupção da ligação, mas sem reduzir a segurança da utilização da Internet.

Por defeito, o limite de tempo de armazenamento temporário para fragmentos de ficheiros é de um segundo. Ao aumentar este valor ou ao desactivar o limite de tempo de armazenamento temporário, isso conduzirá a melhores verificações de vírus, mas atrasará o acesso ao objecto.

Para definir um limite de tempo de armazenamento temporário para fragmentos de ficheiros, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela **Antivírus de Internet** que se abre, na secção **Optimização da verificação**, assinale / desmarque a caixa **Limitar o tempo de armazenamento a** e insira o tempo (em segundos) no campo à direita da caixa.

RESTAURAR AS PREDEFINIÇÕES DE PROTECÇÃO DA INTERNET

Ao configurar o Antivírus de Internet, pode sempre restaurar as respectivas definições recomendadas. Estas são consideradas óptimas, recomendadas pela Kaspersky Lab e agrupadas no nível de segurança **Recomendado**.

Para restaurar as predefinições do Antivírus de Internet, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Na secção **Nível de Segurança**, clique no botão **Nível predefinido** para a componente seleccionada.

PROTEGER O TRÁFEGO DE PROGRAMAS DE MENSAGENS INSTANTÂNEAS

Para além das funcionalidades adicionais para navegar confortavelmente na Internet, os clientes de mensagens instantâneas (a seguir referidos como *clientes de MI*), que actualmente são muito utilizados, têm causado ameaças potenciais à segurança dos computadores. As mensagens que contêm URLs para sites suspeitos e aquelas utilizadas por intrusos para ataques de phishing podem ser transferidas através de clientes de MI. Os programas maliciosos utilizam os clientes de MI para enviar mensagens de spam e URLs para programas (ou os próprios programas), que roubam números de ID e passwords dos utilizadores.

A componente *Antivírus de MI* foi concebida para garantir o funcionamento seguro dos clientes de MI. Esta protege a informação que entra no seu computador através dos protocolos de MI.

O produto garante o funcionamento seguro de várias aplicações de mensagens instantâneas, incluindo o ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Agente Mail.Ru e IRC.

As aplicações Yahoo! Messenger e Google Talk utilizam o protocolo SSL. Para que o Antivírus de MI verifique o tráfego destas aplicações, é necessário utilizar a verificação de ligações encriptadas (ver página 109). Para o fazer, assinale a caixa **Verificar ligações encriptadas** na secção **Rede**.

O tráfego é verificado com base num determinado conjunto de definições. Se forem detectadas ameaças numa mensagem, o Antivírus de MI substitui esta mensagem por uma mensagem de aviso para o utilizador.

O nível de protecção do seu tráfego de MI é determinado por um grupo de definições. As definições podem ser decompostas nos seguintes grupos:

- definições que criam o âmbito de protecção;
- definições que determinam os métodos de verificação.

Para editar a configuração do Antivírus de MI, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de MI**.
3. Faça as alterações necessárias na configuração da componente que seleccionou.

NESTA SECÇÃO:

Algoritmo de funcionamento da componente 67

Criar um âmbito de protecção 67

Seleccionar o método de verificação 68

Utilizar a Análise Heurística 68

ALGORITMO DE FUNCIONAMENTO DA COMPONENTE

O Kaspersky Anti-Virus inclui uma componente que assegura a verificação de mensagens transferidas através de clientes de MI (mensagens instantâneas) quanto à presença de objectos perigosos: *Antivírus de MI*. Este é carregado quando inicia o seu sistema operativo e é executado na memória RAM do seu computador, verificando todas as mensagens recebidas e enviadas.

Por defeito, a protecção do tráfego de clientes de MI é executada através do seguinte algoritmo:

1. Cada mensagem recebida ou enviada pelo utilizador é interceptada pela componente.
2. O Antivírus de MI verifica a mensagem quanto à presença de objectos perigosos ou URLs listados nas bases de dados de endereços de Internet suspeitos e/ou endereços de phishing. Se for detectada uma ameaça, o texto da mensagem será substituído por uma mensagem de aviso para o utilizador.
3. Se não for detectada nenhuma ameaça de segurança na mensagem, esta ficará disponível para utilização pelo utilizador.

Os ficheiros transferidos através de clientes de MI são verificados pela componente Antivírus de Ficheiros (ver secção "Protecção do sistema de ficheiros do computador" na página 42) quando se tentar guardá-los.

CRIAR UM ÂMBITO DE PROTECÇÃO

O âmbito de protecção é entendido como o tipo de mensagens sujeitos a verificação.

- **Mensagens de entrada e de saída**. Por defeito, o Antivírus de MI verifica quer as mensagens de entrada, quer as mensagens de saída.
- **Apenas mensagens de entrada**. Se tiver a certeza de que as mensagens que está a enviar não podem conter objectos perigosos, seleccione esta configuração. O Antivírus de MI apenas verificará mensagens de entrada.

Por defeito, o Kaspersky Anti-Virus verifica quer as mensagens de entrada, quer as mensagens de saída dos clientes de MI.

Se tiver a certeza de que as mensagens que está a enviar não podem conter objectos perigosos, você pode desactivar a verificação do tráfego de saída.

Para desactivar a verificação das mensagens enviadas, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de MI**.
3. Na secção **Âmbito de Protecção**, seleccione a opção **Apenas mensagens de entrada** para a componente seleccionada.

SELECCIONAR O MÉTODO DE VERIFICAÇÃO

Os métodos de verificação consistem na verificação de URLs em mensagens de clientes de MI para determinar se estão incluídos na lista de endereços de Internet suspeitos e/ou lista de endereços de phishing.

- **Verificar se URLs estão listados na base de endereços de Internet suspeitos**. O Antivírus de MI irá verificar os links dentro das mensagens para identificar se estão incluídos na lista negra.
- **Verificar se URLs estão listados na base de endereços de phishing**. As bases de dados do Kaspersky Anti-Virus incluem todos os sites actualmente conhecidos como sendo usados para ataques de phishing. A Kaspersky Lab complementa esta lista com endereços obtidos através do Anti-Phishing Working Group, que é uma organização internacional. Esta lista é actualizada quando actualiza as bases de dados do Kaspersky Anti-Virus.

Para verificar links em mensagens através da base de endereços de Internet suspeitos, execute as seguintes acções

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de MI**.
3. Na secção **Métodos de verificação**, assinale a caixa **Verificar se URLs estão listados na base de endereços de Internet suspeitos** para a componente seleccionada.

Para verificar links em mensagens através da base de endereços de phishing, execute as seguintes acções

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de MI**.
3. Na secção **Métodos de verificação**, assinale a caixa **Verificar se URLs estão listados na base de endereços de phishing** para a componente seleccionada.

UTILIZAR A ANÁLISE HEURÍSTICA

Em termos básicos, o método heurístico analisa as actividades do objecto no sistema. Para esse fim, qualquer script incluído numa mensagem de um cliente de MI é executado num ambiente protegido. Se a actividade deste script for típica de objectos maliciosos, é provável que o objecto seja classificado como malicioso ou suspeito. Por defeito, a análise heurística está activada.

O Kaspersky Anti-Virus irá notificá-lo quando for detectado um objecto malicioso numa mensagem.

Adicionalmente, você pode definir o nível de detalhe para as verificações: **nível superficial**, **nível médio**, ou **nível aprofundado**. Para o fazer, ajuste a barra indicadora para a posição seleccionada.

Para activar/desactivar a análise heurística e para definir o nível de detalhe para a verificação, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de MI**.
3. Na secção **Métodos de verificação**, assinale / desmarque a caixa **Análise heurística** e por baixo defina o nível de detalhe para a componente seleccionada.

DEFESA PROACTIVA

O Kaspersky Anti-Virus protege-o não só de ameaças conhecidas, mas também o protege de ameaças recentes, para as quais não existe qualquer informação nas bases de dados da aplicação. Esta característica é assegurada por uma componente especialmente desenvolvida para esse efeito: a *Defesa Proactiva*.

As tecnologias preventivas fornecidas pela Defesa Proactiva neutralizam as novas ameaças antes de estas terem danificado o seu computador. Em contraste com as tecnologias reactivas, que analisam código com base nos registos das bases de dados do Kaspersky Anti-Virus, as tecnologias preventivas reconhecem uma nova ameaça no seu computador, através de uma sequência de acções executadas por um programa. Se, após a análise de actividades, a sequência de acções da aplicação for suspeita, o Kaspersky Anti-Virus bloqueia a actividade desta aplicação.

➡ *Para editar a configuração da Defesa Proactiva, execute as seguintes acções:*

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Defesa Proactiva**.
3. Faça as alterações necessárias na configuração da componente que seleccionou.

NESTA SECÇÃO:

Utilizar a lista de actividades perigosas 69

Alterar a regra de monitorização de actividades perigosas 70

Criar um grupo de aplicações confiáveis 71

Controlo das contas do sistema 71

UTILIZAR A LISTA DE ACTIVIDADES PERIGOSAS

Note que a configuração do controlo de actividades no Kaspersky Anti-Virus com o Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7, Microsoft Windows 7 x64, Microsoft Windows 7 ou Microsoft Windows 7 x64 difere do processo de configuração noutros sistemas operativos.

Especificidades de configuração do controlo da actividade das aplicações no Microsoft Windows XP

O Kaspersky Anti-Virus monitoriza a actividade das aplicações no seu computador. A Defesa Proactiva reage de imediato a uma sequência definida de acções de aplicações. Por exemplo, quando são detectadas acções tais como um programa a copiar-se para os recursos da rede, a pasta de arranque ou o registo do sistema e a enviar cópias de si mesmo, é muito provável que este programa seja um worm. As outras sequências de operações perigosas incluem:

- acções, típicas de programas Trojan;
- tentativas para interceptar o teclado;
- instalação de controlador oculto;
- tentativas para alterar o núcleo do sistema operativo;
- tentativas para criar objectos ocultos e processos com PID negativo;
- tentativas de alteração do ficheiro ANFITRIÕES;
- tentativas para implementar noutros processos;
- rootkits a redireccionar inputs/outputs de dados;
- tentativas de envio de pedidos DNS.

A lista de actividades perigosas é automaticamente adicionada quando o Kaspersky Anti-Virus é actualizado e não pode ser editada. Contudo, você pode desligar a monitorização para uma ou outra actividade perigosa.

Para desligar a monitorização para uma ou outra actividade perigosa:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Defesa Proactiva**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela **Defesa Proactiva** que se abre, desmarque a caixa junto ao nome da actividade que você não deseja monitorizar.

Especificidades de configuração do controlo da actividade das aplicações no Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 ou Microsoft Windows 7 x64

Se o computador estiver a trabalhar com um dos sistemas operativos acima mencionados, então o controlo não se aplicará a cada evento; isto é devido às características particulares destes sistemas operativos. Por exemplo, o controlo não se aplicará aos seguintes tipos de eventos: *intrusão noutro processo*, *envio de dados através de aplicações confiáveis*, *actividades de sistema suspeitas*, *acesso ao armazenamento protegido*.

ALTERAR A REGRA DE MONITORIZAÇÃO DE ACTIVIDADES PERIGOSAS

A lista de actividades perigosas é automaticamente adicionada quando o Kaspersky Anti-Virus é actualizado e não pode ser editada. Você pode:

- desligar a monitorização para uma ou outra actividade perigosa;
- editar a regra que a Defesa Proactiva utiliza quando detecta um actividade perigosa;
- criar uma lista de exclusões (ver página 106), listando as aplicações que contém actividades que você não considera perigosas.

Para alterar a regra:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Defesa Proactiva**.
3. Clique no botão **Configuração** para a componente que seleccionou.
4. Na janela **Defesa Proactiva** que se abre, na secção **Evento**, seleccione o evento desejado, para o qual deseja editar a regra.
5. Configure as definições para o evento seleccionado, utilizando as ligações na secção de descrição da regra:
   - clique na ligação com a acção predefinida e na janela **Seleccionar acção** que se abre, seleccione a acção desejada;
   - clique na ligação com o período de tempo predefinido (não para qualquer tipo de actividade), e na janela **Detecção de processos ocultos** que se abre, especifique o intervalo de verificação para processos ocultos;
   - clique na ligação On / Off para indicar que o relatório sobre a execução da tarefa deve ser criado.

CRIAR UM GRUPO DE APLICAÇÕES CONFIÁVEIS

Pode utilizar a opção para especificar o conjunto de aplicações confiáveis, cujas actividades não serão verificadas pela Defesa Proactiva. As aplicações confiáveis podem incluir as aplicações com uma assinatura digital ou as listadas na base de dados do Kaspersky Security Network.

- *Para que a Defesa Proactiva considere como confiáveis as aplicações com assinatura digital e / ou contidas na base de dados do Kaspersky Security Network e não notifique sobre as suas actividades, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Defesa Proactiva**.
  3. Na secção **Aplicações confiáveis**, assinale a caixa **Aplicações com assinatura digital** e / ou a caixa **Aplicações da base de dados do Kaspersky Security Network** para a componente seleccionada.

CONTROLO DAS CONTAS DO SISTEMA

As contas de utilizadores controlam o acesso ao sistema e identificam o utilizador no seu ambiente de trabalho, o que impede que outros utilizadores corrompam o sistema operativo ou os dados. Os processos do sistema são processos iniciados por contas de utilizadores do sistema.

- *Se deseja que o Kaspersky Anti-Virus monitorize a actividade dos processos do sistema, para além dos processos de utilizadores:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Defesa Proactiva**.
  3. Na secção **Adicional**, assinale a caixa **Monitorizar contas de utilizadores do sistema** para a componente seleccionada.

VERIFICAÇÃO DO COMPUTADOR

Verificar a existência de vírus no computador é uma das tarefas mais importantes para garantir a segurança do computador. A verificação de vírus detecta a propagação de código malicioso, que por alguma razão não tenha sido detectado pela protecção contra software malicioso. A verificação de vulnerabilidades detecta vulnerabilidades em software que podem ser usadas por intrusos para espalhar objectos maliciosos e obter acesso às informações pessoais.

A Kaspersky Lab distingue as tarefas de verificação de vírus (ver página 72), incluindo a verificação de discos removíveis (ver página 78) e a verificação de vulnerabilidades do sistema e das aplicações (ver página 83).

Para alterar as configurações de qualquer tarefa de verificação:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**, **Verificação de Vulnerabilidade**).
3. Faça as alterações necessárias na configuração da tarefa que seleccionou.

NESTA SECÇÃO:

Verificação de vírus 72

Verificação de vulnerabilidades 83

VERIFICAÇÃO DE VÍRUS

A Kaspersky Lab distingue várias tarefas de verificação de vírus:

- **Verificação de Objectos**. São verificados os objectos seleccionados pelo utilizador. Pode verificar qualquer objecto no sistema de ficheiros do computador. No âmbito desta tarefa pode configurar as definições para a verificação de discos removíveis.
- **Verificação Completa**. Uma verificação minuciosa de todo o sistema. Por defeito, são verificados os seguintes objectos: memória do sistema, programas carregados ao iniciar, cópia de segurança do sistema, bases de dados de e-mail, discos rígidos, meios de armazenamento removíveis e unidades de rede.
- **Verificação Rápida**. São verificados os objectos de inicialização do sistema operativo.

As tarefas Verificação Completa e Verificação Rápida são tarefas específicas. Não é aconselhável que altere a lista de objectos verificados por estas tarefas.

Cada tarefa de verificação é executada na zona especificada e pode ser iniciada de acordo com o agendamento criado. Um conjunto de parâmetros da tarefa de verificação de vírus define o nível de segurança. Por defeito, são fornecidos três níveis.

Depois da tarefa de verificação de vírus começar, o seu progresso é apresentado na secção **Verificação** da janela principal da aplicação, no campo por baixo do nome da tarefa iniciada. Se for detectada uma ameaça, a aplicação executa a acção especificada.

Ao procurar ameaças, a informação sobre os resultados é registada num relatório do Kaspersky Anti-Virus.

Para além disso, você pode seleccionar um objecto a verificar, utilizando as ferramentas padrão do sistema operativo Microsoft Windows, por exemplo, numa janela do **Explorador** ou no seu **Ambiente de Trabalho**, etc. Coloque o cursor sobre o nome do objecto desejado, abra o menu de contexto do Microsoft Windows, clicando com o botão direito do rato, e seleccione a opção **Verificar Vírus**.

Figura 9. Menu de contexto do Microsoft Windows

Também pode visualizar o relatório de verificação, o qual contém informação completa sobre os eventos que ocorreram durante a execução da tarefa.

VEJA TAMBÉM:

Iniciar a tarefa de verificação de vírus 74

Criar um atalho para a execução de tarefas 75

Criar uma lista de objectos a verificar 75

Alterar o nível de segurança 76

Alterar as acções a executar com objectos detectados 76

Alterar o tipo de objectos a verificar 77

Optimização da verificação 78

Verificar discos removíveis 78

Verificação de ficheiros compostos 79

Tecnologia de verificação 80

Alterar o método de verificação 80

Modo de execução: criar um agendamento 81

Modo de execução: especificar uma conta de utilizador 82

Características da inicialização de tarefas agendadas 82

Restaurar as predefinições de verificação 82

INICIAR A TAREFA DE VERIFICAÇÃO DE VÍRUS

Uma tarefa de verificação de vírus pode ser iniciada através de uma das seguintes formas:

- a partir do menu de contexto do Kaspersky Anti-Virus (ver secção "Menu de contexto" na página 38);
- a partir da janela principal (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39) do Kaspersky Anti-Virus;
- através de um atalho existente (ver página 75).

A informação sobre a execução da tarefa será apresentada na janela principal do Kaspersky Anti-Virus.

Para além disso, pode seleccionar um objecto a verificar com as ferramentas padrão do sistema operativo Microsoft Windows (por exemplo, na janela do programa **Explorer** ou no seu **Ambiente de Trabalho**, etc.).

Figura 10. Menu de contexto do Microsoft Windows

Para iniciar a tarefa através de um atalho:

1. Abra a pasta na qual foi criado um atalho.
2. Inicie a tarefa, clicando duas vezes sobre o atalho. A informação sobre a execução da tarefa será apresentada na janela principal do Kaspersky Anti-Virus, na secção **Verificação**.

Para iniciar uma tarefa de verificação de vírus a partir do menu de contexto da aplicação:

1. Clique com o botão direito do rato no ícone da aplicação na área de notificação da barra de tarefas.
2. Seleccione o item **Verificação de vírus** no menu de contexto que se abre.
3. Na janela principal do Kaspersky Anti-Virus que se abre, na secção **Verificação**, clique no botão com o nome da tarefa desejada.

Para iniciar a verificação completa do computador, seleccione o item **Verificação Completa** no menu de contexto. Isso irá iniciar uma verificação completa do computador. A informação sobre a execução da tarefa será apresentada na janela principal do Kaspersky Anti-Virus, na secção **Verificação**.

Para iniciar a tarefa de verificação de vírus a partir da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Na parte esquerda da janela, seleccione a secção **Verificação**.
3. Clique no botão com o nome da tarefa desejada.

Para iniciar uma tarefa de verificação de vírus para um objecto seleccionado a partir do menu de contexto do Microsoft Windows:

1. Clique com o botão direito do rato sobre o nome do objecto seleccionado.
2. Seleccione o item **Verificar Vírus** no menu de contexto que se abre. O progresso e resultados da execução da tarefa serão apresentados na janela que se abre.

CRIAR UM ATALHO PARA A EXECUÇÃO DE TAREFAS

A aplicação fornece a opção de criar atalhos para uma inicialização rápida das tarefas de verificação rápida e de verificação completa. Isto permite iniciar a tarefa de verificação desejada, sem ter de abrir a janela principal da aplicação ou o menu de contexto.

Para criar um atalho para a inicialização de tarefas de verificação, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a secção **Verificação**.
3. Na parte direita da janela, na secção **Execução rápida de tarefas de verificação**, clique no botão **Criar atalho** junto ao nome da tarefa desejada (**Verificação Rápida** ou **Verificação Completa**).
4. Especifique o caminho para guardar um atalho e o respectivo nome na janela que se abre. Por defeito, o atalho é criado com o nome de uma tarefa na pasta *O Meu Computador* do actual utilizador do computador.

CRIAR UMA LISTA DE OBJECTOS A VERIFICAR

Cada tarefa de verificação de vírus tem a sua própria lista de objectos predefinida. Estes objectos podem incluir itens no sistema de ficheiros do computador, tais como discos lógicos e **bases de dados de e-mail** ou outros tipos de objectos, tais como unidades de rede. Você pode editar esta lista.

Os objectos aparecerão na lista, imediatamente, depois de os adicionar. Se a caixa **Incluir subpastas** tiver sido seleccionada quando adicionou o objecto, a verificação será executada de forma recursiva.

Para apagar um objecto da lista, seleccione o objecto e clique na ligação **Apagar**.

Os objectos predefinidos na lista não podem ser editados ou apagados.

Para além de apagar os objectos da lista, também pode ignorá-los, temporariamente, quando executar uma verificação. Para o fazer, seleccione o objecto na lista e desmarque a caixa à esquerda do nome do objecto.

Se o âmbito de verificação estiver vazio ou se não contiver nenhum objecto seleccionado, a tarefa de verificação sob pedido não pode ser iniciada!

Para criar uma lista de objectos para uma tarefa de verificação de objectos, execute as seguintes acções:

1. Abra a janela principal da aplicação.
2. Na parte esquerda da janela, seleccione a secção **Verificação**.
3. Clique na ligação **Adicionar**.
4. Na janela **Seleccionar objecto a verificar** que se abre, seleccione um objecto e clique no botão **Adicionar**. Depois de ter adicionado todos os objectos que necessita, clique no botão **OK**. Para excluir quaisquer objectos da lista de objectos a verificar, desmarque as caixas junto aos mesmos.

Para criar a lista de objectos para as tarefas de verificação rápida ou verificação completa, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa **Verificação Completa** (**Verificação Rápida**).
3. Na secção **Âmbito de verificação**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela **<Nome da tarefa de verificação>: lista de objectos** que se abre, crie a lista utilizando as ligações **Adicionar**, **Editar**, **Apagar**. Para excluir quaisquer objectos da lista de objectos a verificar, desmarque as caixas junto aos mesmos.

ALTERAR O NÍVEL DE SEGURANÇA DO TRÁFEGO DE HTTP

O nível de segurança é uma configuração predefinida das definições de verificação Os especialistas da Kaspersky Lab distinguem três níveis de segurança. Você deve decidir sobre o nível de segurança a seleccionar, com base nas suas próprias preferências. Pode seleccionar um dos seguintes níveis de segurança:

- **Elevado**. Este nível deve estar activado, se suspeita que o seu computador têm uma elevada probabilidade de ser infectado.
- **Recomendado**. Este nível é adequado na maioria dos casos e é recomendado pelos especialistas da Kaspersky Lab.
- **Baixo**. Se está a utilizar aplicações que requerem recursos significativos da memória RAM, seleccione o nível de segurança Baixo porque neste modo a aplicação coloca menos pressão sobre os recursos do sistema.

Se nenhum dos níveis de segurança predefinidos responder às suas necessidades, você pode configurar por si próprio as definições de verificação. Como resultado, o nome do nível de segurança alterar-se-á para **Configurações Personalizadas**. Para restaurar as predefinições de verificação, seleccione um dos níveis de segurança predefinidos.

Para alterar o nível de segurança definido, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Nível de Segurança**, defina o nível de segurança desejado para a tarefa seleccionada.

ALTERAR AS ACÇÕES A EXECUTAR COM OBJECTOS DETECTADOS

Se for detectada uma ameaça, o Kaspersky Anti-Virus atribui-lhe um dos seguintes estados:

- programa malicioso (tais como, um *vírus* ou um *Trojan*);
- estado de *potencialmente infectado* quando a verificação não consegue determinar se o objecto está infectado. Isto ocorre quando a aplicação detectou no ficheiro uma secção de código de um vírus desconhecido ou código alterado de um vírus conhecido.

Se o Kaspersky Anti-Virus detectar objectos infectados ou potencialmente infectados durante uma verificação de vírus, você será notificado sobre isso. Você deve reagir a uma nova ameaça, seleccionando uma acção a executar com o objecto. O Kaspersky Anti-Virus selecciona a opção **Perguntar o que fazer** como a acção a executar com um objecto detectado, a qual é a configuração predefinida. Você pode alterar a acção. Por exemplo, você tem a certeza de que deveria tentar desinfectar cada objecto detectado e não deseja seleccionar a acção **Desinfectar** sempre que recebe uma notificação sobre a detecção de um objecto infectado ou suspeito. Neste caso, deve seleccionar a seguinte acção: **Não perguntar o que fazer. Desinfectar**.

Antes de tentar desinfectar ou apagar um objecto infectado, o Kaspersky Anti-Virus cria uma cópia de segurança do mesmo para permitir o seu restauro ou desinfecção posterior.

Se estiver a trabalhar em modo automático (ver secção "Passo 2. Seleccionar um modo de protecção" na página 28), o Kaspersky Anti-Virus aplicará automaticamente a acção recomendada pelos especialistas da Kaspersky Lab quando forem detectados objectos perigosos. Para objectos maliciosos a acção será **Desinfectar. Apagar se não for possível desinfectar**, enquanto para objectos suspeitos a acção é – **Ignorar**.

Para alterar a acção especificada a executar com objectos detectados:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Acção**, especifique a acção desejada para a tarefa seleccionada.

ALTERAR O TIPO DE OBJECTOS A VERIFICAR

Ao especificar o tipo de objectos a verificar, você estabelece quais os formatos e tamanhos de ficheiros que serão verificados quando a tarefa de verificação seleccionada for executada.

Ao seleccionar os tipos de ficheiro, deve lembrar-se das seguintes características:

- A probabilidade de penetração de código malicioso em diversos formatos de ficheiro (tais como *.txt*) e posterior activação é relativamente reduzida. Por outro lado, existem formatos de ficheiros que contém ou podem conter código executável (tais como *.exe*, *.dll*, *.doc).* O risco de penetração e activação do código malicioso nesses ficheiros é relativamente elevado.
- Lembre-se que um intruso pode enviar um vírus para o seu computador num ficheiro com a extensão *.txt*, que pode na realidade ser um ficheiro executável renomeado como um ficheiro *.txt*. Se seleccionou a opção **Ficheiros verificados por extensão**, a verificação ignoraria tal ficheiro. Se a opção **Ficheiros verificados por formato** for seleccionada, a protecção de ficheiros iria analisar o cabeçalho do ficheiro e determinar que o ficheiro é um ficheiro .exe. Esse ficheiro seria verificado, de forma minuciosa, quanto à existência de vírus.

Para alterar o tipo de objectos a verificar:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Âmbito**, na secção **Tipos de ficheiros**, seleccione a configuração desejada.

OPTIMIZAÇÃO DA VERIFICAÇÃO

Você pode encurtar a duração das verificações e aumentar a velocidade da aplicação. Isto pode ser conseguido, verificando apenas os ficheiros novos e ficheiros que foram alterados desde a última vez que foram verificados. Este modo aplica-se aos ficheiros simples e compostos.

Para além disso, pode reduzir o tempo de verificação para cada ficheiro individual. Depois de excedido o período de tempo especificado, a verificação do ficheiro será interrompida.

Para verificar apenas os ficheiros novos e os ficheiros modificados:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Âmbito**, na secção **Optimização da verificação**, assinale a caixa **Verificar apenas os ficheiros novos e modificados**.

Para impor um limite de tempo à duração da verificação:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Âmbito**, na secção **Optimização da verificação**, assinale a caixa **Ignorar ficheiros cuja verificação demore mais de** e especifique a duração da verificação no campo junto a essa caixa.

VERIFICAR DISCOS REMOVÍVEIS

Actualmente, tornaram-se cada vez mais frequentes os objectos maliciosos que utilizam as vulnerabilidades do sistema operativo para se multiplicarem através das redes e dos meios removíveis.

Utilize a opção para verificar discos removíveis quando estes forem ligados ao computador. Para o fazer, tem de seleccionar uma das acções a serem executadas pelo Kaspersky Anti-Virus:

- **Não verificar**. Os meios removíveis não são, automaticamente, verificados quando forem ligados ao computador.
- **Perguntar ao Utilizador**. Por defeito, o Kaspersky Anti-Virus solicita ao utilizador a acção adicional quando os meios removíveis estão a ser ligados.
- **Verificação Completa**. Quando os discos removíveis forem ligados, a aplicação executa uma verificação completa dos ficheiros armazenados nos mesmos, de acordo com as configurações da tarefa Verificação Completa.
- **Verificação Rápida**. Quando os discos removíveis forem ligados, todos os ficheiros serão verificados de acordo com as configurações da tarefa Verificação Rápida.

- *Para usar a funcionalidade de verificação dos meios removíveis quando forem ligados, execute os seguintes passos:*

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a secção **Verificação**.
3. Na secção **Verificar discos removíveis quando forem ligados**, seleccione a acção e no campo por baixo defina, se necessário, o tamanho máximo do disco a verificar.

VERIFICAÇÃO DE FICHEIROS COMPOSTOS

Um método comum de ocultar vírus é incorporá-los em ficheiros compostos: arquivos, bases de dados, etc. Para detectar vírus que estão ocultos dessa forma, tem de se descompactar um ficheiro composto, o que pode reduzir significativamente a velocidade da verificação.

Para cada tipo de ficheiro composto, pode seleccionar para verificação todos os ficheiros ou apenas os ficheiros novos. Para o fazer, utilize a ligação junto ao nome do objecto. Esta muda de valor quando clica sobre a mesma com o botão esquerdo do rato. Se seleccionar o modo para verificar apenas os ficheiros novos e modificados (ver página 78), não poderá seleccionar o tipo de ficheiros compostos a verificar.

Você pode restringir o tamanho máximo dos ficheiros compostos a verificar. Os ficheiros compostos com um tamanho superior ao valor especificado não serão verificados.

Os ficheiros extensos extraídos a partir de arquivos serão verificados, mesmo se a opção **Não descompactar ficheiros compostos extensos** estiver seleccionada.

- *Para alterar a lista de ficheiros compostos verificados:*

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Âmbito**, na secção **Verificação de ficheiros compostos**, seleccione o tipo desejado de ficheiros compostos a verificar.

- *Para definir o tamanho máximo de ficheiros compostos a verificar:*

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Âmbito**, na secção **Verificação de ficheiros compostos**, clique no botão **Adicional**.
5. Na janela **Ficheiros compostos** que se abre, assinale a caixa **Não descompactar ficheiros compostos extensos** e especifique o tamanho máximo do ficheiro no campo por baixo.

TECNOLOGIA DE VERIFICAÇÃO

Também pode especificar a tecnologia que será utilizada durante a verificação: Pode seleccionar uma das seguintes tecnologias:

- **iChecker**. Esta tecnologia pode aumentar a velocidade de verificação, excluindo determinados objectos da verificação. Um objecto é excluído da verificação, utilizando um algoritmo especial que toma em consideração a data de distribuição das bases de dados da aplicação, a data em que o objecto foi verificado pela última vez e as alterações às definições de verificação.

  Por exemplo, você tem um arquivo ao qual foi atribuído o estado *não infectado* pelo Kaspersky Anti-Virus após a verificação. Na próxima vez, a aplicação irá ignorar este arquivo, excepto se tiver sido alterado ou se as definições de verificação tiverem sido alteradas. Se a estrutura do arquivo tiver sido alterada devido a um novo objecto adicionado ao mesmo, se as definições de verificação tiverem sido alteradas ou se as bases de dados da aplicação tiverem sido actualizadas, a aplicação irá verificar novamente o arquivo.

  Existem limitações no iChecker: não funciona com ficheiros extensos e apenas se aplica a objectos com uma estrutura que a aplicação reconheça (por exemplo, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

- **iSwift**. Esta tecnologia é um desenvolvimento da tecnologia iChecker para computadores que usam sistemas de ficheiros NTFS. Existem limitações no iSwift: está limitada a um local específico no sistema de ficheiros e só pode ser aplicada a objectos num sistema de ficheiros NTFS.

➧ *Para alterar a tecnologia de verificação de objectos:*

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.

2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).

3. Na secção **Nível de Segurança**, clique no botão **Configuração** para a tarefa seleccionada.

4. Na janela que se abre, no separador **Adicional**, na secção **Tecnologias de verificação**, seleccione o modo desejado.

ALTERAR O MÉTODO DE VERIFICAÇÃO

Você pode editar as definições de verificação que determinam o nível de detalhe da verificação. Por defeito, está sempre activado o modo que utiliza os registos da base de dados da aplicação para procurar ameaças. Para além disso, pode aplicar vários métodos de verificação e tecnologias de verificação (ver página 80).

O modo de verificação no qual o Kaspersky Anti-Virus compara o objecto encontrado com os registos da base de dados denomina-se de *análise de assinaturas* e aplica-se sempre à verificação. Para além disso, pode sempre utilizar a *análise heurística*. Este método assume a análise das acções executadas por um objecto no sistema. Se essas acções forem típicas de objectos maliciosos, é provável que o objecto seja classificado como malicioso ou suspeito.

Adicionalmente, pode seleccionar o nível de detalhe para a análise heurística: **nível superficial**, **nível médio**, ou **nível aprofundado**. Para o fazer, ajuste a barra indicadora para a posição seleccionada.

Para além destes métodos de verificação, também pode utilizar a verificação de processos ocultos. Os processos ocultos (rootkits) são conjuntos de ferramentas que podem esconder programas maliciosos no seu sistema operativo. Estes utilitários infiltram-se no sistema, escondendo a sua presença e a presença de processos, pastas e as chaves de registo de outros programas maliciosos instalados com o rootkit. Se a verificação estiver activada, pode especificar o nível detalhado (análise aprofundada) para a detecção de processos ocultos, o qual procurará, cuidadosamente, estes programas, analisando um elevado número de vários objectos.

Para especificar o método de verificação a utilizar:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Modo de execução**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Adicional**, na secção **Métodos de verificação**, seleccione os valores desejados para as definições.

MODO DE EXECUÇÃO CRIAR UM AGENDAMENTO

Você pode criar um agendamento para iniciar as tarefas de verificação de vírus automaticamente.

O principal aspecto a escolher é o intervalo de tempo entre inicializações de tarefas. Para alterar a frequência, especifique as definições de agendamento para a opção seleccionada.

Se não for possível iniciar a tarefa por algum motivo (por exemplo, o computador não estava ligado naquela altura), pode configurar a tarefa para ser automaticamente iniciada assim que for possível.

Para editar um agendamento para as tarefas de verificação:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Modo de execução**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Modo de execução**, na secção **Agendamento**, seleccione a opção **Manualmente** se desejar iniciar uma tarefa de verificação à hora mais adequada. Se deseja que a tarefa seja executada periodicamente, seleccione **Agendamento** e crie um agendamento de execução da tarefa.

Para configurar a execução automática de tarefas ignoradas:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Modo de execução**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Modo de execução**, na secção **Agendamento**, assinale a caixa ☑ **Executar tarefas ignoradas**.

MODO DE EXECUÇÃO ESPECIFICAR UMA CONTA DE UTILIZADOR

Você pode especificar uma conta que será utilizada pela aplicação ao executar uma verificação de vírus.

Para especificar uma conta de utilizador:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Modo de execução**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Modo de execução**, na secção **Utilizador**, assinale a caixa **Executar tarefa como**. Especifique o nome de utilizador e a password.

CARACTERÍSTICAS DA INICIALIZAÇÃO DE TAREFAS AGENDADAS

Todas as tarefas de verificação podem ser iniciadas manualmente ou de acordo com um agendamento.

As tarefas agendadas possuem uma funcionalidade adicional. Por exemplo, você pode *pausar a verificação agendada quando a protecção de ecrã estiver inactiva e o computador estiver desbloqueado*. Esta funcionalidade adia a execução da tarefa até que o utilizador tenha acabado o seu trabalho no computador. Assim, a tarefa de verificação não irá consumir recursos do sistema durante o trabalho.

Para iniciar as tarefas de verificação apenas quando o computador já não está a ser utilizado, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Modo de execução**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Modo de execução**, na secção **Agendamento**, assinale a caixa **Pausar verificação agendada quando a protecção de ecrã estiver inactiva e o computador estiver desbloqueado**.

RESTAURAR AS PREDEFINIÇÕES DE VERIFICAÇÃO

Ao configurar as definições das tarefas, pode sempre restaurar as recomendadas. Estas são consideradas óptimas, recomendadas pela Kaspersky Lab e agrupadas no nível de segurança **Recomendado**.

Para restaurar as predefinições da verificação de ficheiros:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**).
3. Na secção **Nível de Segurança**, clique no botão **Nível predefinido** para a tarefa seleccionada.

VERIFICAÇÃO DE VULNERABILIDADES

A tarefa de verificação de vulnerabilidades consiste em diagnósticos de segurança e na procura de potenciais vulnerabilidades, normalmente utilizadas por intrusos para danificar computadores.

Ao verificar a existência de vulnerabilidades, a aplicação analisa o sistema e procura anomalias e danos nas configurações do sistema operativo e do navegador de Internet. Os diagnósticos de segurança abrangem muitas dimensões, incluindo: a procura de instalações de processos ocultos ou Rootkits (ou seja, programas para monitorizar, de forma secreta, um sistema pirateado), a procura de serviços e configurações vulneráveis e a recolha de informação sobre processos e controladores.

O diagnóstico de vulnerabilidades do sistema pode demorar algum tempo. Quando o diagnóstico é concluído, a informação recolhida é analisada para avaliar problemas de segurança, em termos de possíveis ameaças ao sistema.

Todos os problemas detectados na etapa de análise do sistema serão agrupados com base no nível de perigo que representam. A Kaspersky Lab oferece um conjunto de acções para cada grupo de problemas, as quais ajudam a eliminar vulnerabilidades e pontos fracos nas configurações do sistema. Existem três grupos de problemas e, respectivamente, três grupos de acções associados aos mesmos:

- *Acções vivamente recomendadas* ajudam a eliminar problemas que representam uma séria ameaça de segurança. Recomenda-se que execute todas as acções deste grupo.

- *Acções recomendadas* ajudam a eliminar problemas que representam uma potencial ameaça. Recomenda-se que também execute todas as acções deste grupo.

- *Acções adicionais* ajudam a reparar danos no sistema, que não representam uma ameaça actualmente, mas que podem ameaçar a segurança do computador no futuro.

O resultado da procura de potenciais vulnerabilidades no sistema operativo e nas aplicações de utilizador instaladas está representado por ligações directas para correcções críticas (actualizações da aplicação).

Após o início da tarefa de verificação de vulnerabilidades (ver página 84), a evolução da sua execução é apresentada na janela principal da aplicação e na janela **Verificação de Vulnerabilidade**, no campo **Conclusão**. As vulnerabilidades detectadas ao verificar o sistema e as aplicações são apresentadas na mesma janela, nos separadores **Vulnerabilidades do sistema** e **Aplicações vulneráveis**.

Ao procurar ameaças, a informação sobre os resultados é registada num relatório do Kaspersky Anti-Virus.

Na secção **Verificação de Vulnerabilidade**, na janela de configuração da aplicação, pode definir um agendamento de inicialização (ver página 85) e criar uma lista de objectos a verificar para uma tarefa de verificação de vulnerabilidades (ver página 84), tal como acontece com as tarefas de verificação de vírus. Por defeito, as aplicações já instaladas no computador são seleccionadas como objectos de verificação.

VEJA TAMBÉM:

Iniciar a tarefa de verificação de vulnerabilidades 84

Criar um atalho para a execução de tarefas 84

Criar uma lista de objectos a verificar 84

Modo de execução: criar um agendamento 85

Modo de execução: especificar uma conta de utilizador 86

INICIAR A TAREFA DE VERIFICAÇÃO DE VULNERABILIDADES

A tarefa de verificação de vulnerabilidades pode ser iniciada através de uma das seguintes formas:

- a partir da janela principal (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39) do Kaspersky Anti-Virus;
- através de um atalho existente (ver página 84).

A informação sobre a execução da tarefa será apresentada na janela principal do Kaspersky Anti-Virus e na janela **Verificação de Vulnerabilidade**.

Para iniciar a tarefa através de um atalho:

1. Abra a pasta na qual foi criado um atalho.
2. Inicie a tarefa, clicando duas vezes sobre o atalho. A evolução da tarefa será apresentada na janela principal da aplicação.

Para iniciar a tarefa de verificação de vulnerabilidades a partir da janela da aplicação:

1. Abra a janela principal da aplicação.
2. Na parte esquerda da janela, seleccione a secção **Verificação**.
3. Clique no botão **Abrir janela de Verificação de Vulnerabilidade**.
4. Na janela que se abre, clique no botão **Iniciar Verificação de Vulnerabilidade**. A evolução da execução da tarefa será apresentada no campo **Conclusão**. Clique novamente no botão para parar a execução da tarefa.

CRIAR UM ATALHO PARA A EXECUÇÃO DE TAREFAS

A aplicação fornece a opção de criar um atalho para uma inicialização rápida da tarefa de verificação de vulnerabilidades. Isto permite iniciar a tarefa sem ter de abrir a janela principal da aplicação.

Para criar um atalho para iniciar a tarefa de verificação de vulnerabilidades:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a secção **Verificação**.
3. Na parte direita da janela, na secção **Execução rápida de tarefas de verificação**, clique no botão **Criar atalho** junto ao nome da tarefa (**Verificação de Vulnerabilidade**).
4. Especifique o caminho para guardar um atalho e o respectivo nome na janela que se abre. Por defeito, o atalho é criado com o nome de uma tarefa na pasta *O Meu Computador* do actual utilizador do computador.

CRIAR UMA LISTA DE OBJECTOS A VERIFICAR

A tarefa de verificação de vulnerabilidades tem a sua própria lista predefinida de objectos a verificar. Estes objectos incluem o sistema operativo e os programas instalados no seu computador. Também pode especificar objectos adicionais para verificar: objectos no sistema de ficheiros do computador (por exemplo, discos lógicos, **Bases de dados de e-mail**) ou outros tipos de objectos (por exemplo, unidades de rede).

Os objectos aparecerão na lista, imediatamente, depois de os adicionar. Se a caixa **Incluir subpastas** tiver sido seleccionada quando adicionou o objecto, a verificação será executada de forma recursiva. Os objectos manualmente adicionados também serão verificados quanto à presença de vírus.

Para apagar um objecto da lista, seleccione o objecto e clique na ligação **Apagar**.

Os objectos predefinidos na lista não podem ser editados ou apagados.

Para além de apagar os objectos da lista, também pode ignorá-los, temporariamente, quando executar uma verificação. Para o fazer, seleccione o objecto na lista e desmarque a caixa à esquerda do nome do objecto.

Se o âmbito de verificação estiver vazio ou se não contiver nenhum objecto seleccionado, a tarefa de verificação sob pedido não pode ser iniciada!

Para criar a lista de objectos para uma tarefa de verificação de vulnerabilidades:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa **Verificação de Vulnerabilidade** a secção **Verificação**.
3. Na secção **Âmbito de verificação**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela **Verificação de Vulnerabilidade: lista de objectos** que se abre, crie a lista utilizando as ligações **Adicionar**, **Editar**, **Apagar**. Para excluir, temporariamente, quaisquer objectos da lista de objectos a verificar, desmarque as caixas junto aos mesmos.

MODO DE EXECUÇÃO CRIAR UM AGENDAMENTO

A tarefa de verificação de vulnerabilidades pode ser agendada para ser automaticamente executada.

O principal aspecto a escolher é o intervalo de tempo entre inicializações de tarefas.

Se não for possível iniciar a tarefa por algum motivo (por exemplo, o computador não estava ligado naquela altura), pode configurar a tarefa para ser automaticamente iniciada assim que for possível.

Para editar um agendamento para as tarefas de verificação:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa **Verificação de Vulnerabilidade** a secção **Verificação**.
3. Na secção **Modo de execução**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Modo de execução**, na secção **Agendamento**, seleccione a opção **Manualmente** se desejar iniciar uma tarefa de verificação à hora mais adequada. Se deseja que a tarefa seja executada periodicamente, seleccione **Agendamento** e crie um agendamento de execução da tarefa.

Para configurar a execução automática de tarefas ignoradas:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa **Verificação de Vulnerabilidade** a secção **Verificação**.
3. Na secção **Modo de execução**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Modo de execução**, na secção **Agendamento**, assinale a caixa **Executar tarefas ignoradas**.

MODO DE EXECUÇÃO ESPECIFICAR UMA CONTA DE UTILIZADOR

Você pode especificar uma conta que será utilizada pela aplicação ao executar uma verificação de vulnerabilidades.

Para especificar uma conta de utilizador:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na parte esquerda da janela, seleccione a tarefa **Verificação de Vulnerabilidade** a secção **Verificação**.
3. Na secção **Modo de execução**, clique no botão **Configuração** para a tarefa seleccionada.
4. Na janela que se abre, no separador **Modo de execução**, na secção **Utilizador**, assinale a caixa **Executar tarefa como**. Especifique o nome de utilizador e a password.

ACTUALIZAÇÃO

Manter a aplicação actualizada é um pré-requisito para uma protecção confiável do seu computador. É importante actualizar regularmente a aplicação de forma a manter os seus dados pessoais constantemente protegidos, porque novos vírus, Trojans e novo software malicioso surgem diariamente. A informação sobre ameaças e sobre métodos para as neutralizar está armazenada nas bases de dados do Kaspersky Anti-Virus, por isso a sua actualização atempada é essencial para manter uma protecção fiável.

A componente de actualização da aplicação transfere e instala no seu computador:

- Bases de dados do Kaspersky Anti-Virus.

  A protecção da informação é efectuada através de bases de dados que contêm assinaturas de ameaças e de ataques de rede e os métodos utilizados para os combater. As componentes de protecção utilizam estas bases de dados para procurar e desinfectar objectos perigosos no seu computador. As bases de dados são actualizadas todas as horas com novos registos de novas ameaças. Por isso, recomenda-se que as actualize regularmente.

  Para além das bases de dados do Kaspersky Anti-Virus, também são actualizados os controladores de rede que permitem que as componentes da aplicação interceptem o tráfego de rede.

- Módulos da aplicação.

  Para além das bases de dados do Kaspersky Anti-Virus, também pode actualizar os módulos do programa. Os pacotes de actualização corrigem as vulnerabilidades da aplicação e adicionam novas funcionalidades ou melhoram as já existentes.

Os servidores de actualização da Kaspersky Lab são a principal origem de actualização do Kaspersky Anti-Virus.

Para transferir com sucesso as actualizações a partir dos servidores, o seu computador tem de estar ligado à Internet. Por defeito, as definições da ligação à Internet são automaticamente determinadas. Se as definições do servidor de proxy não forem automaticamente determinadas, as definições de ligação podem ser manualmente configuradas.

Durante uma actualização, as bases de dados e os módulos da aplicação existentes no seu computador são comparados com os disponíveis na origem de actualização. Se o seu computador tiver a última versão das bases de dados e módulos da aplicação, visualizará uma janela de notificação confirmando que a protecção do seu computador está actualizada. Se as bases de dados e módulos existentes no seu computador e no servidor de actualizações diferirem, a aplicação só transferirá as partes que faltam das actualizações. Nem todas as bases de dados e módulos são transferidos, o que aumenta, significativamente, a velocidade de cópia dos ficheiros e poupa tráfego de Internet.

Se as bases de dados estiverem desactualizadas, o pacote de actualização pode ser extenso e isso pode implicar um tráfego adicional de Internet (até várias dezenas de Mb).

Antes de actualizar as bases de dados, o Kaspersky Anti-Virus cria cópias de segurança das mesmas, caso queira reverter para a versão anterior da base de dados.

Poderá precisar da opção de reversão da actualização, por exemplo, se as bases de dados da aplicação ficarem corrompidas durante o processo de actualização. Você pode facilmente reverter para a versão anterior e tentar actualizar novamente as bases de dados.

Ao actualizar o Kaspersky Anti-Virus, você pode copiar as actualizações recolhidas para uma origem local. Este serviço permite actualizar as bases de dados e os módulos do programa em computadores ligados em rede para poupar no tráfego de Internet.

Também pode configurar o início automático da actualização.

A secção **Actualizações** da janela principal da aplicação apresenta informação sobre o actual estado das bases de dados do Kaspersky Anti-Virus:

- data e hora de lançamento;
- número de registos das bases de dados e sua composição;
- estado das bases de dados (actualizadas, desactualizadas ou corrompidas).

Você pode ver o relatório de actualização, que contém informação completa sobre os eventos ocorridos durante a execução da tarefa de actualização (a ligação **Relatório**). Também pode ver o relatório da actividade de vírus em: www.kaspersky.com, clicando na ligação **Relatório de actividade de vírus**.

NESTA SECÇÃO:

Iniciar a Actualização 88

Reverter a última actualização 89

Seleccionar uma origem de actualização 89

Usar um servidor de proxy 90

Configurações regionais 90

Acções após a actualização 90

Actualizar a partir de uma pasta local 91

Alterar o modo de execução da tarefa de actualização 92

Executar actualizações com outra conta de utilizador 92

INICIAR A ACTUALIZAÇÃO

Pode iniciar o processo de actualização em qualquer altura. As actualizações são transferidas a partir da origem de actualização que seleccionou (ver secção "Seleccionar uma origem de actualização" na página 89).

Pode actualizar o Kaspersky Anti-Virus utilizando um dos dois métodos suportados:

- a partir do menu de contexto (ver secção "Menu de contexto" na página 38);
- a partir da janela principal (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39).

A informação sobre a actualização será apresentada na secção **Actualizações** da janela principal da aplicação.

Para iniciar a actualização do Kaspersky Anti-Virus a partir do menu de contexto:

1. Clique com o botão direito do rato no ícone da aplicação na área de notificação da barra de tarefas.
2. Seleccione o item **Actualização** a partir do menu suspenso.

Para iniciar a actualização do Kaspersky Anti-Virus a partir da janela principal da aplicação:

1. Abra a janela principal da aplicação.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Iniciar actualização**. A evolução da tarefa será apresentada na janela principal da aplicação.

REVERTER A ÚLTIMA ACTUALIZAÇÃO

No início do processo de actualização, o Kaspersky Anti-Virus cria uma cópia de segurança das actuais bases de dados e módulos da aplicação. Isto permite que a aplicação continue a funcionar com as bases de dados anteriores, caso a actualização falhe.

A opção de reversão é útil se, por exemplo, as bases de dados ficarem parcialmente corrompidas. As bases de dados locais podem ser corrompidas pelo utilizador ou por um programa malicioso, algo que só é possível se a autodefesa (ver secção "Autodefesa do Kaspersky Anti-Virus" na página 101) estiver desactivada. Você pode facilmente reverter para as bases de dados anteriores e tentar actualizá-las mais tarde.

Para reverter para a versão anterior da base de dados:

1. Abra a janela principal da aplicação.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Reverter para as bases de dados anteriores**.

SELECCIONAR UMA ORIGEM DE ACTUALIZAÇÃO

Origem de actualização é um recurso que contém actualizações para as bases de dados e os módulos da aplicação do Kaspersky Anti-Virus. As origens de actualizações podem ser servidores de HTTP e FTP, pastas locais ou de rede.

A principal origem de actualizações são os servidores de actualização da Kaspersky Lab. Estes são sites especiais da Internet que contêm as actualizações para as bases de dados e módulos da aplicação para todos os produtos da Kaspersky Lab.

Se não tiver acesso aos servidores de actualização da Kaspersky Lab (por exemplo, o seu computador não está ligado à Internet), pode ligar para a sede da Kaspersky Lab +7 (495) 797-87-00 ou +7 (495) 645-79-39 para pedir informação de contacto dos parceiros Kaspersky Lab que lhe possam fornecer actualizações em disquetes ou unidades ZIP.

Pode copiar as actualizações a partir de um disco amovível e carregá-las num site de FTP ou HTTP ou guardá-los numa pasta local ou da rede.

Ao solicitar actualizações em meios removíveis, por favor especifique se também deseja as actualizações para os módulos da aplicação.

Por defeito, a lista de origens de actualização apenas contém os servidores de actualização da Kaspersky Lab.

Se seleccionou um recurso localizado fora da LAN (Rede de Área Local) como origem de actualização, então necessita de uma ligação à Internet para fazer a actualização.

Se vários recursos são seleccionados como origens de actualização, o Kaspersky Anti-Virus tenta ligar-se a eles um após o outro, começando no topo da lista e irá recolher as actualizações a partir da primeira origem disponível.

Para escolher uma origem de actualização:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Configuração** na secção **Origem da actualização**.
4. Na janela que se abre, no separador **Origem**, clique na ligação **Adicionar**.
5. Seleccione um site FTP ou HTTP ou insira o respectivo endereço IP, nome simbólico ou URL na janela **Seleccionar Origem de actualização** que se abre.

USAR UM SERVIDOR DE PROXY

Se está a utilizar um servidor de proxy para se ligar à Internet, deve editar as respectivas definições.

Para configurar o servidor de proxy, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Configuração** na secção **Origem da actualização**.
4. Na janela que se abre, no separador **Origem**, clique no botão **Servidor de proxy**.
5. Edite as definições do servidor de proxy na janela **Configuração do servidor de proxy** que se abre.

CONFIGURAÇÕES REGIONAIS

Se utilizar os servidores de actualização da Kaspersky Lab como origem de actualização, pode seleccionar a localização optimizada do servidor para transferir actualizações. Os servidores da Kaspersky Lab estão localizados em vários países. Ao escolher o servidor de actualização da Kaspersky Lab mais próximo de si, permitir-lhe-á poupar tempo e efectuará mais rapidamente as transferências de actualizações.

Para escolher o servidor mais próximo:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Configuração** na secção **Origem da actualização**.
4. Na janela que se abre, no separador **Origem**, na secção **Configurações regionais**, seleccione a opção **Seleccionar na lista** e depois seleccione o país mais próximo da sua actual localização a partir da lista suspensa.

   Se seleccionar a opção **Detectar automaticamente**, então a informação sobre a sua localização será copiada do registo do seu sistema operativo quando a actualização estiver a decorrer.

ACÇÕES APÓS A ACTUALIZAÇÃO

O Kaspersky Anti-Virus também lhe permite especificar as acções a executar automaticamente após a actualização. Estão disponíveis as seguintes acções possíveis:

- **Verificar novamente a quarentena**. A área da quarentena contém objectos que foram marcados pela aplicação como suspeitos ou possivelmente infectados. Possivelmente, após a actualização da base de dados, o produto conseguirá reconhecer a ameaça de forma clara e neutralizá-la. É possível que, após a actualização da base de dados, a aplicação consiga identificar e eliminar a ameaça. Por essa razão, a aplicação verifica os objectos da quarentena após cada actualização. A verificação pode alterar o estado dos objectos. Alguns objectos podem então ser restaurados para as localizações anteriores e poderá continuar a trabalhar com eles.

- **Copiar actualizações para a pasta**. Se os computadores estão ligados através de uma rede doméstica de área local, não é necessário transferir e instalar actualizações em cada um dos computadores, separadamente. Você pode utilizar o serviço de distribuição de actualizações para poupar na largura de banda, uma vez que o serviço garante que as actualizações só são transferidas uma única vez.

Para verificar os ficheiros da quarentena após a actualização:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Assinale a caixa **Verificar novamente a quarentena após a actualização** na secção **Adicional**.

ACTUALIZAR A PARTIR DE UMA PASTA LOCAL

O procedimento de recolha das actualizações a partir de uma pasta local funciona da seguinte forma:

1. Um dos computadores da rede recolhe o pacote de actualização do Kaspersky Anti-Virus a partir dos servidores da Kaspersky Lab ou a partir de um servidor-espelho que aloja um conjunto de actualizações correntes. As actualizações recolhidas são colocadas numa pasta partilhada.
2. Os outros computadores da rede acedem à pasta partilhada para recolher as actualizações do Kaspersky Anti-Virus.

Para activar o modo de distribuição das actualizações:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Assinale a caixa **Copiar actualizações para a pasta** na secção **Adicional** e no campo por baixo especifique caminho da pasta pública para a qual serão copiadas todas as actualizações transferidas. Também pode seleccionar o caminho na janela que é apresentada quando clica no botão **Procurar**.

Se deseja que as actualizações sejam efectuadas a partir da pasta de acesso público seleccionada, execute estas acções em todos os computadores da rede:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Configuração** na secção **Origem da actualização**.
4. Na janela que se abre, no separador **Origem**, clique na ligação **Adicionar**.
5. Na janela **Seleccionar Origem de actualização** que se abre, seleccione uma pasta ou insira o caminho completo para a mesma no campo **Origem**.
6. Desmarque a caixa **Servidores de actualização da Kaspersky Lab** no separador **Origem**.

ALTERAR O MODO DE EXECUÇÃO DA TAREFA DE ACTUALIZAÇÃO

O modo de execução da tarefa de actualização do Kaspersky Anti-Virus é seleccionado no assistente de configuração da aplicação (ver secção "Passo 3. Configurar as actualizações da aplicação" na página 28). Se desejar alterar o modo de execução seleccionado para a actualização, você pode reconfigurá-lo.

A tarefa de actualização pode ser iniciada através de um dos seguintes modos:

- **Automaticamente**. O Kaspersky Anti-Virus verifica, em intervalos especificados, se existem actualizações na origem de actualização. A frequência dessa verificação pode aumentar durante surtos de vírus e diminuir quanto não existirem surtos. Se forem encontradas novas actualizações, o programa transfere-as e instala-as no computador.
- **Planificadas** (o intervalo de tempo muda dependendo das definições). As actualizações serão automaticamente executadas com base no agendamento criado.
- **Manualmente**. Se seleccionar esta opção, você executará as actualizações do Kaspersky Anti-Virus manualmente.

Para configurar o agendamento de execução da tarefa de actualização:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Configuração** na secção **Modo de execução**.
4. Na janela que se abre, no separador **Modo de execução**, seleccione o modo de execução da tarefa de actualização na secção **Agendamento**. Se a opção **Planificadas** estiver seleccionada, crie o agendamento.

   Se uma actualização for ignorada por algum motivo (por exemplo, o computador não estava ligado naquela altura), pode configurar a tarefa para ser automaticamente iniciada assim que for possível. Para o fazer, seleccione a caixa **Executar tarefas ignoradas** na parte inferior da janela. Esta caixa está disponível para todas as opções de agendamento, excepto para as opções **Horas**, **Minutos** e **Após inicialização da aplicação**.

EXECUTAR ACTUALIZAÇÕES COM OUTRA CONTA DE UTILIZADOR

Por defeito, o procedimento de actualização é executado com a sua conta do sistema. Contudo, o Kaspersky Anti-Virus pode ser actualizado a partir de uma origem para a qual você não tem direitos de acesso (por exemplo, uma pasta de rede que contenha as actualizações) ou credenciais de utilizador de proxy autorizado. Pode executar a actualização da aplicação com a conta de um utilizador que possua os direitos necessários.

Para iniciar a actualização com uma conta de utilizador diferente:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Configuração** na secção **Modo de execução**.
4. Na janela que se abre, no separador **Modo de execução**, na secção **Utilizador**, assinale a caixa **Executar tarefa como**. Especifique o nome de utilizador e a password.

CONFIGURAÇÃO DAS DEFINIÇÕES DA APLICAÇÃO

A janela de configuração da aplicação é utilizada para o acesso rápido às principais configurações do Kaspersky Anti-Virus.

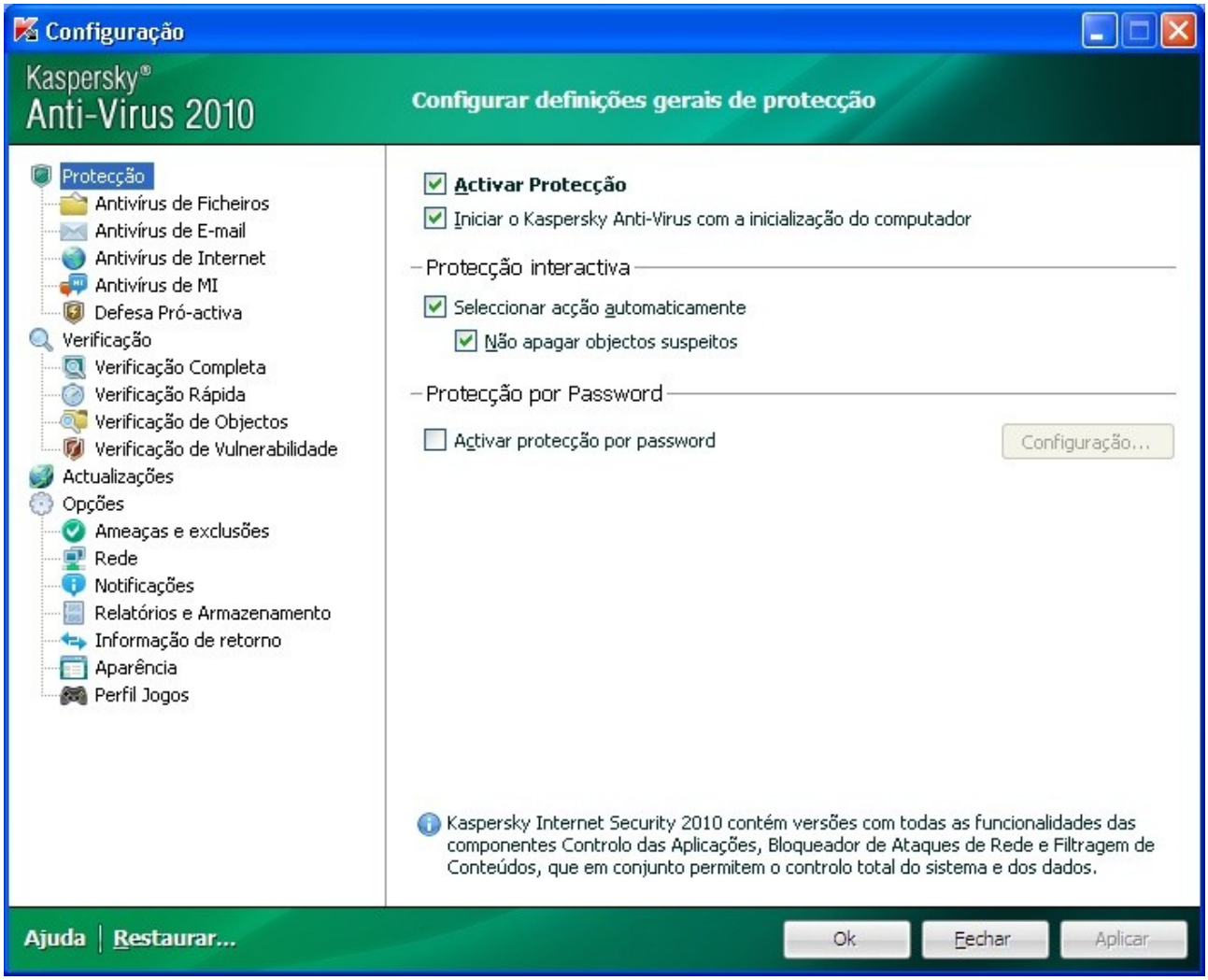


Figura 11. Janela de configuração da aplicação

A janela de configuração da aplicação consiste em duas partes:

- a parte esquerda da janela permite o acesso às componentes do Kaspersky Anti-Virus, às tarefas de verificação de vírus, às tarefas de actualização, etc.;
- a parte direita da janela contém uma lista de configurações para a componente, tarefa, etc. seleccionada na parte esquerda da janela.

Você pode abrir esta janela:

- A partir da janela principal (ver secção "Janela principal do Kaspersky Anti-Virus" na página 39). Para o fazer, clique na ligação **Configuração** na parte superior da janela principal.
- A partir do menu de contexto (ver secção "Menu de contexto" na página 38). Para o fazer, seleccione o item **Configuração** no menu de contexto da aplicação.

Figura 12. Menu de contexto

NESTA SECÇÃO:

Protecção 94
Antivírus de Ficheiros 97
Antivírus de E-mail 97
Antivírus de Internet 98
Antivírus de MI 99
Defesa Proactiva 99
Verificação 100
Actualização 101
Configuração 101

PROTECÇÃO

Na janela **Protecção** pode utilizar as seguintes funções adicionais do Kaspersky Anti-Virus:

- Activar / desactivar a protecção do Kaspersky Anti-Virus (ver página 95).
- Iniciar o Kaspersky Anti-Virus com a inicialização do sistema operativo (ver página 95).
- Utilizar o modo de protecção interactiva (ver página 96).
- Restringir o acesso ao Kaspersky Anti-Virus (ver página 96).

ACTIVAR / DESACTIVAR A PROTECÇÃO DO COMPUTADOR

Por defeito, o Kaspersky Anti-Virus é iniciado quando o sistema operativo é carregado e protege o seu computador até este ser desligado. Todas as componentes de protecção estão em execução.

Você pode desactivar, por completo ou parcialmente, a protecção fornecida pelo Kaspersky Anti-Virus.

Os especialistas da Kaspersky Lab recomenda vivamente que **não desactive a protecção**, uma vez que isso poderia levar à infecção do seu computador e à perda de dados.

Quando desactiva a protecção, todas as suas componentes ficam inactivas. Isto é indicado pelos seguintes sinais:

- ícone da aplicação inactivo (a cinzento) (ver secção "Ícone da área de notificação" na página 37) na área de notificação da barra de ferramentas;
- cor vermelha do indicador de segurança.

Neste caso, a protecção é abordada no contexto das componentes de protecção. Desactivar ou pausar componentes de protecção não afecta a execução das tarefas de verificação de vírus e das actualizações do Kaspersky Anti-Virus.

Para desactivar, por completo, a protecção:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre seleccione a secção **Protecção**.
3. Desmarque a caixa **Activar Protecção**.

INICIAR O KASPERSKY ANTI-VIRUS COM A INICIALIZAÇÃO DO SISTEMA OPERATIVO

Se, por alguma razão, tiver que encerrar o Kaspersky Anti-Virus por completo, seleccione o item **Sair** no menu de contexto
(ver secção "Menu de contexto" na página 38) do Kaspersky Anti-Virus. Como resultado, a aplicação irá descarregar-se da memória RAM.
Isto significa que o seu computador estará a funcionar desprotegido.

Você pode reactivar a protecção do computador, iniciando o Kaspersky Anti-Virus a partir do menu **Iniciar →Programas →Kaspersky Anti-Virus 2010 →Kaspersky Anti-Virus 2010**.

A protecção também pode ser automaticamente retomada, depois de reiniciar o seu sistema operativo.

Para activar este modo:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre seleccione a secção **Protecção**.
3. Assinale a caixa **Iniciar o Kaspersky Anti-Virus com a inicialização do computador**.

UTILIZAR O MODO DE PROTECÇÃO INTERACTIVA

O Kaspersky Anti-Virus utiliza dois modos para interagir com o utilizador:

- *Modo de Protecção Interactiva*. O Kaspersky Anti-Virus notifica o utilizador sobre todos os eventos perigosos e suspeitos ocorridos no sistema. Neste modo, o utilizador decide, por si próprio, se deseja permitir ou bloquear as acções.

- *Modo de Protecção Automática*. O Kaspersky Anti-Virus aplicará, automaticamente, as acções recomendadas pela Kaspersky Lab em resposta a eventos perigosos.

Para utilizar o modo de protecção automática:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.

2. Na janela que se abre seleccione a secção **Protecção**.

3. Na secção **Protecção interactiva**, assinale a caixa **Seleccionar acção automaticamente**. Se não pretende que o Kaspersky Anti-Virus apague os objectos suspeitos ao trabalhar em modo automático, assinale a caixa **Não apagar objectos suspeitos**.

RESTRINGIR O ACESSO AO KASPERSKY ANTI-VIRUS

Um computador pessoal pode ser utilizado por diversos utilizadores, incluindo aqueles com diferentes níveis de conhecimentos informáticos. Deixar aberto o acesso ao Kaspersky Anti-Virus e às suas configurações poderia reduzir, significativamente, a segurança de todo o computador.

Para aumentar o nível de segurança do seu computador, utilize uma password para aceder ao Kaspersky Anti-Virus. Você pode bloquear todas as operações do Kaspersky Anti-Virus, com excepção das notificações sobre a detecção de objectos perigosos ou impedir que as seguintes acções sejam executadas:

- alteração das definições da aplicação;

- encerramento da aplicação.

Para proteger o acesso ao Kaspersky Anti-Virus com uma password, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.

2. Na janela que se abre seleccione a secção **Protecção**.

3. Na secção **Protecção por password,** assinale a caixa **Activar protecção por password** e clique no botão **Configuração**.

4. Na janela **Protecção por password** que se abre, insira a password e especifique a área que será abrangida pela restrição de acesso. Agora sempre que algum utilizador no seu computador tentar executar as acções que seleccionou, o Kaspersky Anti-Virus irá sempre pedir a password.

ANTIVÍRUS DE FICHEIROS

As configurações da componente Antivírus de Ficheiros estão agrupadas na janela (ver secção "Protecção do sistema de ficheiros do computador" na página 42). Pode executar as seguintes acções, editando as configurações:

- desactivar o Antivírus de Ficheiros;
- alterar o nível de segurança (ver página 44);
- alterar as acções a executar com objectos detectados (ver página 45);
- criar um âmbito de protecção (ver página 45);
- optimizar a verificação (ver página 47);
- configurar a verificação de ficheiros compostos (ver página 47);
- alterar o modo de verificação (ver página 48);
- utilizar a análise heurística (ver página 46);
- pausar a componente (ver página 49);
- seleccionar uma tecnologia de verificação (ver página 49);
- restaurar as predefinições de protecção (ver página 51), caso tenham sido alteradas.

Para desactivar o Antivírus de Ficheiros, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.

   Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.

   Desmarque a caixa **Activar Antivírus de Ficheiros** na parte direita da janela.

Para continuar para a configuração do Antivírus de Ficheiros, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Ficheiros**.
3. Na parte direita da janela, seleccione as configurações da componente para o nível de segurança e reacção à ameaça.
   Clique no botão **Configuração** para aceder às outras configurações do Antivírus de Ficheiros.

ANTIVÍRUS DE E-MAIL

As configurações da componente Antivírus de E-mail estão agrupadas na janela (ver secção "Protecção de E-mails" na página 52). Pode executar as seguintes acções, editando as configurações:

- desactivar o Antivírus de E-mail;
- alterar o nível de segurança (ver página 54);
- alterar as acções a executar com objectos detectados (ver página 54);
- criar um âmbito de protecção (ver página 55);
- utilizar a análise heurística (ver página 57);
- configurar a verificação de ficheiros compostos (ver página 57);
- configurar condições de filtragem para objectos anexados ao e-mail (ver página 58);
- restaurar as predefinições da protecção de e-mail (ver página 58).

Para desactivar o Antivírus de E-mail, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
3. Desmarque a caixa **Activar Antivírus de E-mail** na parte direita da janela.

Para continuar para a configuração do Antivírus de E-mail, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de E-mail**.
3. Na parte direita da janela, seleccione as configurações da componente para o nível de segurança e reacção à ameaça. Clique no botão **Configuração** para aceder às outras configurações do Antivírus de E-mail.

ANTIVÍRUS DE INTERNET

As configurações da componente Antivírus de Internet estão agrupadas na janela (ver secção "Protecção do Tráfego de Internet" na página 59). Pode executar as seguintes acções, editando as configurações:

- desactivar o Antivírus de Internet;
- alterar o nível de segurança (ver página 61);
- alterar as acções a executar com objectos detectados (ver página 61);
- criar um âmbito de protecção (ver página 62);
- alterar os métodos de verificação (ver página 62);
- utilizar o Conselheiro de URLs da Kaspersky (ver página 63);
- optimizar a verificação (ver página 64);
- utilizar a análise heurística (ver página 64);
- restaurar as predefinições do Antivírus de Internet (ver página 65).

Para desactivar o Antivírus de Internet, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Desmarque a caixa **Activar Antivírus de Internet** na parte direita da janela.

Para continuar para a configuração do Antivírus de Internet, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de Internet**.
3. Na parte direita da janela, seleccione as configurações da componente para o nível de segurança e reacção à ameaça.
   Clique no botão **Configuração** para aceder às outras configurações do Antivírus de Internet.

ANTIVÍRUS DE MI

As configurações da componente Antivírus de MI estão agrupadas na janela (ver secção "Proteger o tráfego de programas de mensagens instantâneas" na página 66). Pode executar as seguintes acções, editando as configurações:

- desactivar o Antivírus de MI;
- criar um âmbito de protecção (ver página 67);
- alterar o método de verificação (ver página 68);
- utilizar a análise heurística (ver página 68);

Para desactivar o Antivírus de MI, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de MI**.
3. Desmarque a caixa **Activar Antivírus de MI** na parte direita da janela.

Para continuar para a configuração do Antivírus de MI, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Antivírus de MI**.
3. Na parte direita da janela, faça as alterações necessárias na configuração da componente.

DEFESA PROACTIVA

Esta janela agrupa as configurações da componente Defesa Proactiva. Pode executar as seguintes acções, editando as configurações:

- desactivar a Defesa Proactiva;
- gerir a lista de actividades perigosas;
- alterar a reacção da aplicação face a actividades perigosas no sistema (ver página 70);
- criar um grupo de aplicações confiáveis (ver página 71);
- monitorizar contas de utilizadores do sistema (ver página 71).

Para desactivar a Defesa Proactiva, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Defesa Proactiva**.
3. Desmarque a caixa **Activar Defesa Proactiva** na parte direita da janela.

Para continuar para a edição das configurações da Defesa Proactiva, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, na secção **Protecção**, seleccione a componente **Defesa Proactiva**.
3. Na parte direita da janela, faça as alterações necessárias na configuração da componente.

VERIFICAÇÃO

A selecção do método a utilizar para verificar objectos no seu computador é determinada pelo conjunto de propriedades atribuídas a cada tarefa.

A Kaspersky Lab distingue as tarefas de verificação de vírus e as tarefas de verificação de vulnerabilidades. As tarefas de verificação de vírus incluem o seguinte:

- **Verificação de Objectos**. Verifica objectos seleccionados pelo utilizador. Pode verificar qualquer objecto no sistema de ficheiros do computador.
- **Verificação Completa**. Uma verificação minuciosa de todo o sistema. Por defeito, são verificados os seguintes objectos: memória do sistema, programas carregados ao iniciar, cópia de segurança do sistema, bases de dados de e-mail, discos rígidos, meios de armazenamento removíveis e unidades de rede.
- **Verificação Rápida**. Verificação de vírus dos objectos de inicialização do sistema operativo.

Pode executar as seguintes acções na janela de configuração de cada tarefa de verificação de vírus:

- seleccionar o nível de segurança com as configurações relevantes que definem o comportamento da tarefa no momento da execução;
- seleccionar a acção que a aplicação aplicará quando detectar um objecto infectado/potencialmente infectado;
- criar um agendamento para executar as tarefas automaticamente;
- criar uma lista de objectos a verificar (para as tarefas de verificação rápida e de verificação completa);
- especificar os tipos de ficheiros a analisar em termos de vírus;
- especificar as definições da verificação de ficheiros compostos;
- seleccionar os métodos de verificação e as tecnologias de verificação.

Na secção **Verificação**, pode especificar as configurações para a verificação automática de discos removíveis quando estes forem ligados ao computador, e criar atalhos para a inicialização rápida das tarefas de verificação de vírus e de verificação de vulnerabilidades.

Na janela de configuração, pode executar as seguintes acções para uma tarefa de verificação de vulnerabilidades:

- criar um agendamento para executar as tarefas automaticamente;
- criar uma lista de objectos a verificar.

Para editar as definições das tarefas:

1. Abra a janela de configuração da aplicação.
2. Na parte esquerda da janela, seleccione a tarefa desejada na secção **Verificação** (**Verificação Completa**, **Verificação Rápida**, **Verificação de Objectos**, **Verificação de Vulnerabilidade**).
3. Configure as definições na parte direita da janela.

ACTUALIZAÇÃO

A actualização do Kaspersky Anti-Virus é executada de acordo com um conjunto de parâmetros.

Você pode executar as seguintes acções na janela de configuração da tarefa de actualização:

- alterar o endereço do recurso a partir do qual as actualizações da aplicação serão distribuídas e instaladas;
- especificar o tipo de modo, de acordo com o qual o processo de actualização da aplicação será iniciado;
- definir o agendamento de execução para uma tarefa;
- especificar a conta com a qual a actualização será iniciada;
- seleccionar as acções que devem ser executadas depois da actualização da aplicação.

Para aceder à configuração das actualizações:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Seleccione a secção **Actualizações** na parte esquerda da janela.
3. Seleccione o modo de execução desejado na parte direita da janela e seleccione uma origem de actualização. Configure outras definições da tarefa na secção **Adicional**.

CONFIGURAÇÃO

Através da janela **Configuração** pode utilizar as seguintes funções adicionais do Kaspersky Anti-Virus:

- Autodefesa do Kaspersky Anti-Virus (ver página 101).
- Utilização da tecnologia de desinfecção avançada (ver página 102).
- Serviço de poupança da bateria (ver página 102).
- Adiar a execução da tarefa de verificação de vírus caso esta conduza ao funcionamento lento de outras aplicações (ver página 103).
- Exportar / importar as definições do Kaspersky Anti-Virus (ver página 103).
- Restaurar as predefinições do Kaspersky Anti-Virus (ver página 104).

AUTODEFESA DO KASPERSKY ANTI-VIRUS

O Kaspersky Anti-Virus garante a segurança do seu computador contra programas maliciosos e por isso pode ser o alvo de programas maliciosos que tentam bloquear ou apagá-lo.

Para assegurar a fiabilidade do sistema de segurança do seu computador, o Kaspersky Anti-Virus é fornecido com funcionalidades de autodefesa e de protecção contra o acesso remoto.

Nos computadores com sistemas operativos de 64-bit e com o Microsoft Windows Vista, a autodefesa apenas está disponível para impedir que os ficheiros do próprio Kaspersky Anti-Virus nas unidades locais e o registo do sistema sejam alterados ou apagados.

Enquanto se utiliza a protecção do acesso remoto, é frequente surgirem situações em que os programas de administração remota (por exemplo, RemoteAdmin) são necessários. Para assegurar o seu normal desempenho, deve adicionar estes programas à lista de aplicações confiáveis e activar a opção **Não monitorizar a actividade das aplicações** para os mesmos.

Para activar os mecanismos de autodefesa do Kaspersky Anti-Virus, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Opções**.
3. Na secção **Autodefesa**, assinale a caixa **Activar Autodefesa** para implementar os mecanismos de protecção do Kaspersky Anti-Virus contra alterações ou eliminação dos seus próprios ficheiros do disco rígido, dos processos da memória RAM e dos registo do sistema.

   Na secção **Autodefesa**, assinale a caixa **Desactivar Serviço de Controlo Externo** para bloquear qualquer tentativa para gerir remotamente os serviços da aplicação.

   Se alguma das acções listadas forem tentadas, aparecerá uma mensagem por cima do ícone da aplicação na área de notificação da barra de ferramentas (a não ser que o serviço de notificação tenha sido desactivado pelo utilizador).

TECNOLOGIA DE DESINFECÇÃO AVANÇADA

Actualmente, os programas maliciosos conseguem invadir os níveis mais baixos de um sistema operativo, o que os torna, praticamente, impossíveis de apagar. Se for detectada uma actividade maliciosa no sistema, o Kaspersky Anti-Virus irá sugerir-lhe que execute um procedimento especial de desinfecção avançada que permitirá eliminar a ameaça e apagá-la do computador.

Após este procedimento, terá de reiniciar o seu computador. Depois de reiniciar o computador, recomendamos que execute a verificação completa de vírus.

Para iniciar o procedimento de desinfecção avançada, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Opções**.
3. Na secção **Compatibilidade**, assinale a caixa **Activar Tecnologia de Desinfecção Avançada**.

UTILIZAR O KASPERSKY ANTI-VIRUS NUM COMPUTADOR PORTÁTIL

Para poupar energia num computador portátil, as tarefas de verificação de vírus podem ser adiadas.

Uma vez que as verificações de vírus e as actualizações muitas vezes exigem uma quantidade significativa de recursos e tempo, recomendamos que desactive a inicialização agendada destas tarefas. Isso permitirá poupar a carga da bateria. Se necessário, você pode actualizar o Kaspersky Anti-Virus ou iniciar uma verificação de vírus por si próprio.

Para utilizar o serviço de poupança da bateria, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Opções**.
3. Na secção **Compatibilidade**, assinale a caixa **Desactivar verificações agendadas quando o computador estiver a funcionar com bateria**.

DESEMPENHO DO COMPUTADOR DURANTE A EXECUÇÃO DE TAREFAS

As tarefas de verificação de vírus podem ser adiadas para limitar a carga sobre o CPU (Unidade de Processamento Central) e os subsistemas de armazenamento do disco.

A execução das tarefas de verificação aumenta a carga sobre o CPU e os subsistemas do disco, tornando mais lento o funcionamento de outras aplicações. Se isso acontecer, por defeito, o Kaspersky Anti-Virus irá pausar as tarefas de verificação de vírus e libertará recursos do sistema para as aplicações do utilizador.

Contudo, existem algumas aplicações que se irão iniciar logo que os recursos do CPU fiquem disponíveis e que serão executadas em segundo plano. Para que a verificação não dependa do desempenho dessas aplicações, então os recursos do sistema não devem ser concedidos a essas aplicações.

Por favor, note que esta definição pode ser configurada, individualmente, para cada tarefa de verificação. Nesse caso, a configuração seleccionada para uma determinada tarefa terá uma prioridade mais elevada.

- *Para adiar a execução das tarefas de verificação, caso esta conduza ao funcionamento lento de outros programas:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, seleccione a secção **Opções**.
  3. Na secção **Compatibilidade**, assinale a caixa **Conceder recursos para outras aplicações**.

EXPORTAR / IMPORTAR AS DEFINIÇÕES DO KASPERSKY ANTI-VIRUS

O Kaspersky Anti-Virus consegue importar a exportar as respectivas definições

Esta é uma funcionalidade útil quando, por exemplo, o Kaspersky Anti-Virus está instalado no seu computador de casa e no seu trabalho. Você pode configurar a aplicação da forma que pretender em casa, guardar essas definições num ficheiro num disco, usar a funcionalidade de importação e carregá-las no seu computador no trabalho. As definições são armazenadas num ficheiro especial de configuração.

- *Para exportar as actuais definições do Kaspersky Anti-Virus, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, seleccione a secção **Opções**.
  3. Na secção **Gestão das configurações da aplicação**, clique no botão **Guardar**.
  4. Na janela que se abre, insira o nome do ficheiro de configuração e o caminho onde o ficheiro deve ser guardado.

- *Para importar as definições da aplicação a partir de um ficheiro de configuração guardado:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, seleccione a secção **Opções**.
  3. Na secção **Gestão das configurações da aplicação**, clique no botão **Carregar**.
  4. Na janela que se abre, seleccione o ficheiro a partir do qual você pretende importar as definições do Kaspersky Anti-Virus.

RESTAURAR AS PREDEFINIÇÕES

Você pode sempre voltar às definições predefinidas ou recomendadas para o Kaspersky Anti-Virus. Estas são consideradas as definições óptimas e são recomendadas pela Kaspersky Lab. As predefinições são restauradas com o Assistente de Configuração da Aplicação (ver secção "Assistente de Configuração da Aplicação" na página 26).

Na janela que se abre é-lhe pedido que determine quais as definições e para que componentes é que deverão ou não ser guardadas as definições quando for restaurado o nível de segurança recomendado.

A lista contém as componentes do Kaspersky Anti-Virus, cujas definições foram alteradas pelo utilizador. Se tiverem sido criadas definições especiais para alguma das componentes, essas também serão apresentadas na lista.

Estas listas são criadas ao trabalhar com o Kaspersky Anti-Virus no que respeita a tarefas e requisitos de segurança individuais. A criação destas listas demora bastante tempo, por isso recomenda-se que as guarde antes de restaurar as predefinições da aplicação.

Depois de concluir o Assistente de Configuração, o nível de segurança **Recomendado** será definido para todas as componentes, excepto para as definições que você decidiu manter personalizadas ao restaurar. Para além disso, as definições, que especificou ao trabalhar com o Assistente, também serão aplicadas.

➧ *Para restaurar as definições de protecção, execute as seguintes acções:*

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Opções**.
3. Na secção **Gestão das configurações da aplicação**, clique no botão **Restaurar**.
4. Na janela que se abre, assinale as caixas das definições que deseja guardar. Clique no botão **Seguinte**. Isto fará com que o Assistente de Configuração da Aplicação seja executado. Siga as respectivas instruções.

AMEAÇAS E EXCLUSÕES

Na secção **Ameaças e exclusões** da janela de configuração do Kaspersky Anti-Virus você pode efectuar as seguintes acções:

- seleccionar categorias de ameaças detectáveis (ver secção "Seleccionar categorias de ameaças detectáveis" na página 105);
- criar a zona confiável para a aplicação.

Uma *zona confiável* é a lista de objectos, criada pelo utilizador, que não devem ser controlados pela aplicação. Ou seja, é um conjunto de exclusões do âmbito de protecção do Kaspersky Anti-Virus.

Uma zona confiável é criada a partir da lista de aplicações confiáveis (ver secção "Seleccionar aplicações confiáveis" na página 105) e das regras de exclusão (ver secção "Regras de exclusão" na página 106).

O utilizador cria uma zona confiável com base nas especificidades dos objectos com que trabalha e com base nas aplicações instaladas no computador. Você pode precisar de criar uma lista de exclusões se, por exemplo, a aplicação bloquear o acesso a um objecto ou programa e você tiver a certeza de que são absolutamente seguros.

VEJA TAMBÉM:

Seleccionar categorias de ameaças detectáveis 105

Seleccionar aplicações confiáveis 105

Regras de exclusão 106

Máscaras de exclusão de ficheiros permitidas 107

Máscaras de tipo de ameaça permitidas 108

SELECCIONAR CATEGORIAS DE AMEAÇAS DETECTÁVEIS

O Kaspersky Anti-Virus protege-o contra vários tipos de programas maliciosos. Independentemente das definições seleccionadas, a aplicação irá sempre verificar e desinfectar vírus, programas Trojan e utilitários de hackers. Estes programas podem causar danos significativos no seu computador. Para conseguir um maior nível de segurança para o seu computador, você pode alargar a lista de ameaças detectáveis, activando o controlo de diversos programas potencialmente perigosos.

Para seleccionar categorias de ameaças detectáveis, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.

2. Na janela que se abre, seleccione a secção **Ameaças e exclusões**. Clique no botão **Configuração** na secção **Ameaças**.

3. Na janela **Ameaças** que se abre, seleccione as categorias de ameaças em relação às quais deseja proteger o seu computador.

SELECCIONAR APLICAÇÕES CONFIÁVEIS

Você pode criar uma lista de aplicações confiáveis, que permitirá que os respectivos ficheiros e actividades de rede (incluindo as actividades suspeitas) não sejam controlados, assim como as tentativas para aceder ao registo do sistema.

Por exemplo, você acha que os objectos utilizados pelo Microsoft Windows Notepad são seguros e não necessitam de ser verificados. Ou seja, você confia nesta aplicação. Para excluir da verificação os objectos utilizados por este processo, adicione a aplicação Notepad à lista de aplicações confiáveis. Contudo, o ficheiro executável e o processo da aplicação confiável serão verificados, quanto à existência de vírus, tal como antes. Para excluir completamente uma aplicação (da verificação), você deve usar as regras de exclusão.

Para além disso, algumas acções classificadas como perigosas podem ser consideradas como normais para algumas aplicações. Por exemplo, aplicações que alternam automaticamente a disposição do teclado, como o Punto Switcher, normalmente interceptam o texto inserido no seu teclado. Para tomar em consideração as especificidades dessas aplicações e desactivar a monitorização da sua actividade, recomendamos que as adicione à lista de aplicações confiáveis.

A opção de excluir da verificação as aplicações confiáveis permite resolver potenciais problemas de compatibilidade entre a aplicação e outros programas (por exemplo, o problema da dupla verificação do tráfego de rede de um outro computador por parte do Kaspersky Anti-Virus e por outra aplicação antivírus), assim como aumentar o desempenho do computador, o que é crucial quando se utilizam aplicações de servidor.

Por defeito, o Kaspersky Anti-Virus verifica objectos abertos, executados ou guardados por qualquer processo de programa e monitoriza a actividade de todas as aplicações e o tráfego de rede que elas geram.

Para adicionar uma aplicação à lista confiável, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Ameaças e exclusões**.
3. Na secção **Exclusões**, clique no botão **Configuração**.
4. Na janela que se abre, no separador **Aplicações confiáveis**, clique na ligação **Adicionar**.
5. Seleccione uma aplicação no menu que se abre. Depois de seleccionar o item **Procurar**, abrir-se-á uma janela na qual tem de especificar o caminho para o ficheiro executável. Depois de seleccionar o item **Aplicações,** abrir-se-á a lista de aplicações actualmente em execução.
6. Na janela **Exclusões para aplicações** que se abre, especifique as configurações da regra para a aplicação.

Você pode alterar ou apagar a aplicação confiável da lista, utilizando as ligações correspondentes na parte inferior do separador. Para remover uma aplicação da lista sem a apagar, desmarque a caixa junto ao nome da aplicação.

REGRAS DE EXCLUSÃO

Os softwares potencialmente perigosos não têm uma função maliciosa, mas podem ser utilizados como componente auxiliar para um código malicioso, uma vez que contém falhas e erros. Esta categoria inclui, por exemplo, programas de administração remota, clientes de IRC, servidores de FTP, diversos utilitários para parar processos ou escondê-los, keyloggers (registadores de teclas digitadas), decifradores de passwords, autodialers (ligações telefónicas automáticas), etc. Esses programas não são classificados como vírus (not-a-virus). Estes podem ser divididos em diversos tipos, tais como Adware, Jokes, Riskware, etc. (para mais informação sobre programas potencialmente perigosos detectados pela aplicação, veja a Enciclopédia de Vírus em www.viruslist.com). Após a verificação, tais programas podem ser bloqueados. Visto que muitos deles são largamente utilizados pelos utilizadores, você tem a opção de os excluir da verificação.

Por exemplo, você pode usar, frequentemente, um programa de Administrador Remoto. Este é um programa de acesso remoto com o qual você pode trabalhar num computador remoto. O Kaspersky Anti-Virus considera a actividade deste programa como sendo potencialmente perigosa e poderá bloqueá-la. Se não deseja que a aplicação seja bloqueada, você deve criar uma regra de exclusão para a aplicação que é detectada como: *not-a-virus:RemoteAdmin.Win32.RAdmin.22* de acordo com a Enciclopédia de Vírus.

Regras de exclusão são conjuntos de condições que o Kaspersky Anti-Virus utiliza para verificar se pode ignorar a verificação de um objecto.

Você pode excluir da verificação os ficheiros de determinados formatos, utilizando uma máscara de ficheiro, ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objectos, de acordo com a classificação de tipo de ameaça da Enciclopédia de Vírus.

Tipo de ameaça é o estado que o Kaspersky Anti-Virus atribui a um objecto após a verificação. Um estado é atribuído com base na classificação de programas maliciosos e potencialmente perigosos listados na Enciclopédia de Vírus da Kaspersky Lab.

A adição de exclusões cria uma regra que pode ser utilizada por várias componentes da aplicação (tais como Antivírus de Ficheiros (ver secção "Protecção do sistema de ficheiros do computador" na página 42), Antivírus de E-mail (ver secção "Protecção de E-mails" na página 52), Antivírus de Internet (ver secção "Protecção do tráfego de Internet" na página 59), assim como por tarefas de verificação de vírus.

Para criar uma regra de exclusão, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Ameaças e exclusões**.
3. Na secção **Exclusões**, clique no botão **Configuração**.
4. Na janela que se abre, no separador **Regras de exclusão**, clique na ligação **Adicionar**.
5. Na janela **Regra de exclusão** que se abre, edite as definições da regra de exclusão.

VEJA TAMBÉM:

Máscaras de exclusão de ficheiros permitidas 107

Máscaras de tipo de ameaça permitidas 108

MÁSCARAS DE EXCLUSÃO DE FICHEIROS PERMITIDAS

Vamos ver alguns exemplos de máscaras permitidas que pode utilizar quando cria listas de exclusão de ficheiros. Estes são os seguintes:

1. Máscaras sem caminhos de ficheiro:
   - ***.exe** – todos os ficheiros com a extensão *exe*;
   - ***.ex?** – todos os ficheiros com a extensão *ex?*, onde **?** pode representar qualquer caractere único;
   - **teste** – todos os ficheiros com o nome *teste.*
2. Máscaras com caminhos de ficheiro absolutos:
   - **C:\dir*.*** ou **C:\dir*** ou **C:\dir** – todos os ficheiros na pasta *C:\dir*;
   - **C:\dir*.exe** – todos os ficheiros com a extensão exe na pasta *C:\dir*;
   - **C:\dir*.ex?** – todos os ficheiros com a extensão *ex?* na pasta *C:\dir*, onde **?** pode representar qualquer caractere único;
   - **C:\dir\teste** – apenas o ficheiro *C:\dir\teste*.

     Se deseja excluir a verificação de ficheiros em todas as subpastas da pasta especificada, assinale a opção **Incluir subpastas** quando criar uma máscara.
3. Máscaras para caminhos de ficheiro:
   - **dir*.***, ou **dir***, ou **dir** – todos os ficheiros em todas as pastas *dir*;
   - **dir\teste** – todos os ficheiros *teste* incluídos nas pastas *dir*;
   - **dir*.exe** – todos os ficheiros com a extensão *exe* em todas as pastas *dir*;
   - **dir*.ex?** – todos os ficheiros com a extensão *ex?* em todas as pastas *dir*, onde **?** pode representar qualquer caractere único.

     Se deseja excluir a verificação de ficheiros em todas as subpastas da pasta especificada, assinale a opção **Incluir subpastas** quando criar uma máscara.

As máscaras de exclusão *.* e * só podem ser utilizadas, se você especificar o tipo de classificação da ameaça de acordo com a Enciclopédia de Vírus Neste caso, a ameaça especificada não será detectada em nenhum dos objectos. Se utilizar estas máscaras sem especificar o tipo de classificação, basicamente isso significa desactivar a monitorização. Ao definir uma exclusão, recomenda-se que não seleccione como exclusão um caminho relativo a uma unidade de rede (que foi criada com o comando subst com base numa pasta do sistema de ficheiros) ou uma unidade que seja uma réplica de uma pasta de rede. A razão para isso prende-se com o facto de diferentes recursos poderem ter atribuídos o mesmo nome de unidade para diferentes utilizadores, o que irá inevitavelmente resultar no funcionamento incorrecto das regras de exclusão.

MÁSCARAS DE TIPO DE AMEAÇA PERMITIDAS

Quando adiciona ameaças para excluir determinadas ameaças com base na sua classificação da Enciclopédia de Vírus, você pode especificar as seguintes definições:

- O nome completo da ameaça, tal como aparece na Enciclopédia de Vírus presente em *www.viruslist.com* (por exemplo, *not-a-virus:RiskWare.RemoteAdmin.RA.311* ou *Flooder.Win32.Fuxx*).
- O nome da ameaça através da máscara. Por exemplo:
  - **not-a-virus*** – exclui da verificação programas legais, mas potencialmente perigosos, assim como programas de brincadeiras (joke programs);
  - ***Riskware.*** – exclui da verificação o riskware (software potencialmente perigoso);
  - ***RemoteAdmin.*** – exclui da verificação todos os programas de administração remota

REDE

Na secção **Rede** da janela de configuração da aplicação, pode seleccionar as portas monitorizadas pelo Kaspersky Anti-Virus e configurar a verificação de ligações encriptadas:

- criar uma lista de portas monitorizadas;
- activar / desactivar o modo de verificação de ligações encriptadas (utilizando o protocolo SSL) (ver página 109);
- editar as definições do servidor de proxy (ver página 111).

VEJA TAMBÉM:

Criar uma lista de portas monitorizadas 108

Verificar ligações encriptadas 109

Verificar ligações encriptadas no Mozilla Firefox 110

Verificar ligações encriptadas no Opera 111

Configuração do servidor de proxy 111

CRIAR UMA LISTA DE PORTAS MONITORIZADAS

Algumas componentes de protecção, tais como Antivírus de E-mail (ver secção "Protecção de E-mails" na página 52) e Antivírus de Internet
(ver secção "Protecção do tráfego de Internet" na página 59), monitorizam os fluxos de dados transferidos através de determinados protocolos e que passam através de determinadas portas abertas no seu computador. Assim, por exemplo, o Antivírus de E-mail analisa a informação transferida através do protocolo SMTP e o Antivírus de Internet analisa os pacotes HTTP.

Pode seleccionar um de dois modos de monitorização:

- **Monitorizar todas as portas de rede**;
- **Monitorizar apenas as portas seleccionadas**. No pacote da aplicação está incluída uma lista das portas que são utilizadas para transmitir e-mails e tráfego de HTTP.

- *Para adicionar uma porta à lista de portas monitorizadas:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, seleccione a secção **Rede**.
  3. Na secção **Portas monitorizadas** clique no botão **Seleccionar**.
  4. Na janela **Portas de rede** que se abre, clique na ligação **Adicionar**.
  5. Na janela **Porta de rede** que se abre, especifique os dados necessários.

- *Para excluir uma porta da lista de portas monitorizadas:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, seleccione a secção **Rede**.
  3. Na secção **Portas monitorizadas** clique no botão **Seleccionar**.
  4. Na janela **Portas de rede** que se abre, desmarque a caixa junto à descrição da porta.

- *Para criar a lista de aplicações para as quais deseja monitorizar todas as portas, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
  2. Na janela que se abre, seleccione a secção **Rede**.
  3. Na secção **Portas monitorizadas** clique no botão **Seleccionar**.
  4. Na janela **Portas de rede** que se abre, assinale a caixa **Monitorizar todas as portas para as aplicações especificadas** e clique na ligação **Adicionar** na secção por baixo.
  5. Seleccione uma aplicação no menu que se abre. Depois de seleccionar o item **Procurar**, abrir-se-á uma janela na qual tem de especificar o caminho para o ficheiro executável. Depois de seleccionar o item **Aplicações**, abrir-se-á a lista de aplicações actualmente em execução.
  6. Na janela **Aplicação** que se abre, especifique a descrição para a aplicação seleccionada.

VERIFICAR LIGAÇÕES ENCRIPTADAS

A ligação por intermédio do protocolo SSL (Camada Segura de Transferência) protege o canal de intercâmbio de dados através da Internet. O protocolo SSL permite identificar as partes que estão a trocar dados através de certificados electrónicos, codificar os dados a serem transferidos e assegurar a sua integridade durante a transferência.

Estas funcionalidades do protocolo são utilizadas por hackers para espalhar programas maliciosos, uma vez que a maior parte dos programas de antivírus não verifica o tráfego por SSL.

O Kaspersky Anti-Virus verifica as ligações seguras através de um certificado da Kaspersky Lab. Este certificado será sempre utilizado para verificar se a ligação é segura.

Mais tarde, as verificações de tráfego através do protocolo SSL serão executadas com o certificado da Kaspersky Lab instalado. Se for detectado um certificado inválido quando se ligar ao servidor (por exemplo, se o certificado for substituído por um intruso), surgirá uma notificação com uma sugestão para aceitar ou rejeitar o certificado ou para ver a informação sobre o certificado. Se a aplicação estiver a funcionar em modo automático, a ligação através de um certificado inválido será interrompida sem qualquer notificação.

Para activar a verificação de ligações encriptadas, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Rede**.
3. Na janela que se abre, assinale a caixa **Verificar ligações encriptadas** e clique no botão **Instalar certificado**.
4. Na janela que se abre, clique no botão **Instalar certificado**. Isto irá iniciar um assistente com instruções a utilizar para instalar o certificado com sucesso.

A instalação automática do certificado apenas estará disponível no Microsoft Internet Explorer. Para verificar as ligações encriptadas no Mozilla Firefox ou no Opera, deve instalar manualmente o certificado da Kaspersky Lab.

VERIFICAR LIGAÇÕES ENCRIPTADAS NO MOZILLA FIREFOX

O navegador Mozilla Firefox não utiliza o armazenamento de certificados do Microsoft Windows. Para verificar as ligações SSL quando utiliza o Firefox, tem de instalar manualmente o certificado da Kaspersky Lab.

Para instalar o certificado da Kaspersky Lab, execute as seguintes acções:

1. No menu do navegador, seleccione o item **Tools** →**Settings**.
2. Na janela que se abre, seleccione a secção **Additional**.
3. Na secção **Certificates**, seleccione o separador **Security** e clique no botão **Viewing certificates**.
4. Na janela que se abre, seleccione o separador **Certification Centers** e clique no botão **Restore**.
5. Seleccione o ficheiro do certificado da Kaspersky Lab na janela que se abre. O caminho para o ficheiro do certificado da Kaspersky Lab é: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Na janela que se abre, assinale as caixas para seleccionar quais as acções que devem ser verificadas com o certificado instalado. Para ver informação sobre o certificado, use o botão **View**.

Para instalar o certificado da Kaspersky Lab para o Mozilla Firefox version 3.x, execute as seguintes acções:

1. No menu do navegador, seleccione o item **Tools** →**Settings**.
2. Na janela que se abre, seleccione a secção **Additional**.
3. No separador **Encryption**, clique no botão **Viewing certificates**.
4. Na janela que se abre, seleccione o separador **Certification Centers** e clique no botão **Import**.
5. Seleccione o ficheiro do certificado da Kaspersky Lab na janela que se abre. O caminho para o ficheiro do certificado da Kaspersky Lab é: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Na janela que se abre, assinale as caixas para seleccionar quais as acções que devem ser verificadas com o certificado instalado. Para ver informação sobre o certificado, use o botão **View**.

Se o seu computador tiver o Microsoft Windows Vista, o caminho para o ficheiro do certificado da Kaspersky Lab será o seguinte: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

VERIFICAR LIGAÇÕES ENCRIPTADAS NO OPERA

O navegador Opera não utiliza o armazenamento de certificados do Microsoft Windows. Para verificar as ligações SSL quando utiliza o Opera, tem de instalar manualmente o certificado da Kaspersky Lab.

Para instalar o certificado da Kaspersky Lab, execute as seguintes acções:

1. No menu do navegador, seleccione o item **Tools** →**Settings**.
2. Na janela que se abre, seleccione a secção **Additional**.
3. Na parte esquerda da janela, seleccione o separador **Security** e clique no botão **Manage Certificates**.
4. Na janela que se abre, seleccione o separador **Vendors** e clique no botão **Import**.
5. Seleccione o ficheiro do certificado da Kaspersky Lab na janela que se abre. O caminho para o ficheiro do certificado da Kaspersky Lab é: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Na janela que se abre, clique no botão **Install**. O certificado da Kaspersky Lab será então instalado. Para ver informação sobre o certificado e para seleccionar acções para as quais o certificado será utilizado, seleccione o certificado na lista e clique no botão **View**.

Para instalar o certificado da Kaspersky Lab para o Opera versão 9.x, execute as seguintes acções:

1. No menu do navegador, seleccione o item **Tools** →**Settings**.
2. Na janela que se abre, seleccione a secção **Additional**.
3. Na parte esquerda da janela, seleccione o separador **Security** e clique no botão **Manage Certificates**.
4. Na janela que se abre, seleccione o separador **Certification Centers** e clique no botão **Import**.
5. Seleccione o ficheiro do certificado da Kaspersky Lab na janela que se abre. O caminho para o ficheiro do certificado da Kaspersky Lab é: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Na janela que se abre, clique no botão **Install**. O certificado da Kaspersky Lab será então instalado.

Se o seu computador tiver o Microsoft Windows Vista, o caminho para o ficheiro do certificado da Kaspersky Lab será o seguinte: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

CONFIGURAÇÃO DO SERVIDOR DE PROXY

Se a ligação à Internet do computador for efectuada através de um servidor de proxy, você pode precisar de editar as definições de ligação. O Kaspersky Anti-Virus usa estas definições para determinadas componentes de protecção, assim como para actualizar as bases de dados e módulos da aplicação.

Se a sua rede inclui um servidor de proxy que utiliza uma porta diferente do normal, você deve adicionar o número da porta à lista de portas monitorizadas.

Para configurar o servidor de proxy, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Rede**.
3. Na secção **Servidor de proxy**, clique no botão **Configurar o servidor de proxy**.
4. Na janela **Configuração do servidor de proxy** que se abre, altere as definições do servidor de proxy.

NOTIFICAÇÕES

Durante o funcionamento do Kaspersky Anti-Virus, ocorrem diversos tipos de eventos. Estes podem ser de natureza informativa ou podem conter informação importante. Por exemplo, um evento pode informá-lo de que a actualização da aplicação foi concluída com sucesso ou pode registar um erro no funcionamento de uma determinada componente que deve ser imediatamente eliminado.

Para manter-se actualizado sobre os eventos ocorridos no funcionamento do Kaspersky Anti-Virus, utilize o serviço de notificação.

Por defeito, o utilizador é notificado sobre os eventos através de mensagens de pop-up com um sinal áudio.

As notificações podem ser entregues através de uma das seguintes duas formas:

- mensagens de pop-up que aparecem por cima do ícone da aplicação na bandeja do sistema;
- mensagens sonoras;
- mensagens de e-mail.

Para desactivar a entrega de notificações, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Notificações**.
3. Desmarque a caixa **Activar notificações de eventos**.

Mesmo que a entrega de notificações esteja desactivada, ainda assim a informação sobre os eventos ocorridos durante o funcionamento do Kaspersky Anti-Virus será registada no relatório de funcionamento da aplicação.

Para seleccionar o método de entrega de notificações, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Notificações** e clique no botão **Configuração**.
3. Na janela **Notificações** que se abre, seleccione o método de entrega de notificações.

VEJA TAMBÉM:

Desactivar notificações sonoras 112

Entrega de notificações por e-mail 113

DESACTIVAR NOTIFICAÇÕES SONORAS

Por defeito, todas as notificações são acompanhadas por um sinal áudio. O esquema de sons do Microsoft Windows é utilizado para esse fim. A caixa **Usar esquema de sons predefinido do Windows** permite alterar o esquema a utilizar. Se a caixa estiver desmarcada, será utilizado o esquema de sons usado nas versões anteriores da aplicação.

Para desactivar as notificações sonoras, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Notificações**.
3. Desmarque a caixa **Activar notificações sonoras**.

ENTREGA DE NOTIFICAÇÕES POR E-MAIL

Se as notificações forem entregues por e-mail, edite as definições de entrega.

Para configurar as definições de e-mail para a entrega de notificações, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Notificações**.
3. Assinale a caixa **Activar notificações por e-mail** e clique no botão **Configuração de E-mail**.
4. Na janela **Configuração de notificações por e-mail** que se abre, especifique as definições de entrega.

RELATÓRIOS E ARMAZENAMENTO

Esta secção contém as definições que controlam as operações com os ficheiros de dados do Kaspersky Anti-Virus.

Os *ficheiros de dados da aplicação* são objectos que foram colocados na quarentena pelo Kaspersky Anti-Virus ou movidos para a cópia de segurança, assim como ficheiros com relatórios sobre o funcionamento das componentes da aplicação.

Nesta secção você pode:

- editar as definições para a criação (ver página 113) e armazenamento de relatórios (ver página 114);
- editar as definições da quarentena e da cópia de segurança (ver página 116).

VEJA TAMBÉM:

Registar eventos no relatório 113
Limpar os relatórios da aplicação 114
Guardar relatórios 114
Quarentena para objectos potencialmente infectados 114
Cópias de segurança de objectos perigosos 115
Acções com objectos em quarentena 115
Guardar os objectos da quarentena e da cópia de segurança 116
Relatórios 125

REGISTAR EVENTOS NO RELATÓRIO

Você pode adicionar ao relatório informações sobre eventos não críticos, eventos do sistema de ficheiros e eventos do registo. Por defeito, estes eventos não são registados no relatório.

Para adicionar ao relatório as informações sobre eventos não críticos, eventos do sistema de ficheiros e eventos do registo:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Relatórios e Armazenamento**.
3. Na secção **Relatórios**, assinale a caixa desejada.

LIMPAR OS RELATÓRIOS DA APLICAÇÃO

A informação sobre o funcionamento do Kaspersky Anti-Virus é registada nos relatórios. Você pode limpá-los.

➧ *Para limpar os* relatórios*, execute as seguintes acções:*:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Relatórios e Armazenamento**.
3. Na secção **Relatórios**, clique no botão **Limpar**.
4. Na janela **Limpar relatórios** que se abre, assinale as caixas das categorias de relatórios que deseja limpar.

GUARDAR RELATÓRIOS

Você pode determinar o tempo de armazenamento máximo para os relatórios de eventos (a caixa ☑ **Guardar relatórios até**). Por defeito, o tempo máximo é de 30 dias: depois de decorrido este tempo, os objectos serão apagados. Você pode alterar o tempo de armazenamento máximo ou até mesmo limpar quaisquer limites impostos sobre o mesmo. Para além disso, pode especificar o tamanho máximo do ficheiro de relatório (a caixa ☑ **Tamanho máximo dos ficheiros**). Por defeito, o tamanho máximo é de 1024 MB. Quando o tamanho máximo for atingido, o conteúdo do ficheiro será substituído com novos registos. Pode cancelar quaisquer limites definidos para o tamanho do relatório ou inserir um outro valor.

➧ *Para configurar as definições de armazenamento de relatórios, execute as seguintes acções:*

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Relatórios e Armazenamento**.
3. Na janela que se abre, na secção **Relatórios**, assinale as caixas ☑ desejadas e altere o tamanho máximo do relatório e o respectivo tempo de armazenamento, se necessário.

QUARENTENA PARA OBJECTOS POTENCIALMENTE INFECTADOS

A *Quarentena* é uma área de armazenamento especial que contém objectos que poderão estar infectados com vírus.

Os *objectos potencialmente infectados* são objectos que se suspeita estarem infectados com vírus ou modificações de vírus.

Um objecto potencialmente infectado pode ser detectado e colocado em quarentena pelo Antivírus de Ficheiros, Antivírus de E-mail, Defesa Proactiva ou durante uma verificação de vírus.

Os objectos são colocados em quarentena como resultado do funcionamento do Antivírus de Ficheiros e do Antivírus de E-mail, assim como durante uma verificação de vírus, se:

- *O código do objecto analisado é parecido com uma ameaça conhecida mas está parcialmente modificado*.

  As bases de dados do Kaspersky Anti-Virus contêm informação sobre ameaças que já foram estudadas pelos especialistas da Kaspersky Lab. Se um programa malicioso é modificado e estas alterações ainda não foram introduzidas nas bases de dados, o Kaspersky Anti-Virus classifica o objecto infectado com o programa malicioso alterado como um objecto, potencialmente, infectado e indicará a ameaça com a qual esta infecção se assemelha.

- *O código do objecto detectado faz lembrar a estrutura de um programa malicioso. No entanto, não existe nada similar registado nas bases de dados da aplicação*.

  É possível que seja um novo tipo de ameaça, por isso o Kaspersky Anti-Virus classifica o objecto como um objecto, potencialmente, infectado.

Os ficheiros são identificados pelo *analisador do código heurístico* como estando potencialmente infectados com um vírus. Este mecanismo é razoavelmente eficaz e muito raramente conduz a falsos alarmes.

No que respeita à Defesa Proactiva, a componente coloca um objecto em quarentena se, como resultado da análise de comportamento, a sequência de acções do objecto suscitar suspeitas.

Quando coloca um objecto em Quarentena, esse objecto não é copiado, mas sim movido: o objecto é apagado do disco ou e-mail e é guardado na pasta da Quarentena. Os ficheiros em Quarentena são guardados num formato especial e não são perigosos.

É possível que, após a actualização da base de dados, o Kaspersky Anti-Virus consiga identificar a ameaça de forma clara e neutralizá-la. Devido a este facto, a aplicação verifica os objectos da quarentena após cada actualização (ver página 90).

CÓPIAS DE SEGURANÇA DE OBJECTOS PERIGOSOS

Por vezes, quando os ficheiros são desinfectados, a sua integridade perde-se. Se um ficheiro desinfectado contém informação importante e se depois da desinfecção essa informação fica parcial ou completamente inacessível, pode tentar restaurar o objecto original a partir da sua cópia de segurança.

Uma *Cópia de Segurança* é uma cópia do objecto perigoso original, que é criada quando o ficheiro é primeiro desinfectado ou apagado, e é guardada na cópia de segurança.

A *Cópia de Segurança* é uma área de armazenamento especial que contém as cópias de segurança de objectos perigosos após o processamento ou eliminação. A principal função de um armazenamento de cópias de segurança é a capacidade de restaurar o objecto original em qualquer altura. Os ficheiros são guardados na Cópia de Segurança com um formato especial e não são perigosos.

ACÇÕES COM OBJECTOS EM QUARENTENA

Pode executar as seguintes acções com objectos em quarentena:

- mover para a quarentena ficheiros que você suspeita estarem infectados;
- verificar e desinfectar todos os objectos potencialmente infectados na quarentena, utilizando as bases de dados actuais do Kaspersky Anti-Virus;
- restaurar os ficheiros para as pastas a partir das quais foram movidos para a quarentena ou para as pastas seleccionadas pelo utilizador;
- apagar qualquer objecto ou grupo de objectos seleccionados na quarentena;
- enviar o objecto em quarentena à Kaspersky Lab para análise.

Para executar algumas acções com objectos em quarentena:

1. Abra a janela principal da aplicação e clique na ligação **Quarentena**.
2. Execute as acções desejadas na janela que se abre, no separador **Ameaças detectadas**.

GUARDAR OS OBJECTOS DA QUARENTENA E DA CÓPIA DE SEGURANÇA

Pode editar as seguintes definições para a quarentena e cópia de segurança:

- Determine o tempo de armazenamento máximo para os objectos em quarentena e para as cópias de objectos na cópia de segurança (a caixa **Guardar objectos até**). Por defeito, o tempo de armazenamento dos objectos é de 30 dias. Depois de decorrido este tempo, os objectos serão apagados. Você pode alterar o prazo de armazenamento máximo ou remover esta restrição por completo.

- Especifique o tamanho máximo da área de armazenamento de dados (a caixa **Tamanho máximo**). Por defeito, o tamanho máximo é de 100 MB. Pode cancelar o limite do tamanho do relatório ou definir outro valor para o mesmo.

Para configurar as definições da quarentena e da cópia de segurança:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.

2. Na janela que se abre, seleccione a secção **Relatórios e Armazenamento**.

3. Na secção **Quarentena e Cópia de Segurança**, assinale as caixas desejadas e insira o tamanho máximo da área de armazenamento de dados, se necessário.

INFORMAÇÃO DE RETORNO

Todos os dias surgem inúmeras ameaças novas a nível mundial. Para facilitar a recolha de estatísticas sobre novos tipos e origens de ameaças e sobre métodos para a sua eliminação, a Kaspersky Lab convida-o a utilizar o serviço *Kaspersky Security Network*.

A utilização do Kaspersky Security Network sugere o envio de determinadas informações à Kaspersky Lab: Os seguintes dados serão enviados:

- Um identificador único atribuído ao seu computador pela aplicação da Kaspersky Lab. Este identificador caracteriza as configurações de hardware do seu computador e não contêm nenhuma informação privada.

- Informação sobre ameaças detectadas pelas componentes da aplicação. A estrutura e conteúdos da informação depende do tipo de ameaça detectada.

- Informação sobre o sistema operativo: a versão do sistema operativo, pacotes de serviço instalados, serviços e controladores a serem transferidos, versões dos clientes de e-mail e dos navegadores de Internet, extensões do navegador, número da versão instalada da aplicação da Kaspersky Lab.

Para activar o envio de estatísticas no Kaspersky Security Network, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.

2. Na janela que se abre, seleccione a secção **Informação de Retorno**.

3. Assinale a caixa **Aceito participar no Kaspersky Security Network**.

APARÊNCIA DA APLICAÇÃO

Pode mudar a aparência do Kaspersky Anti-Virus, criando e utilizando vários gráficos e esquemas de cores. Também pode configurar a utilização dos vários elementos activos da interface, tais como o ícone da aplicação na área de notificação da barra de ferramentas do Microsoft Windows e as mensagens de pop-up.

VEJA TAMBÉM:

Elementos Activos da Interface 117

Modo de Apresentação da Aplicação 118

ELEMENTOS ACTIVOS DA INTERFACE

Para configurar as definições para os elementos activos da interface (tais como o item do Kaspersky Anti-Virus na bandeja do sistema e as mensagens de pop-up), você pode utilizar as seguintes funcionalidades do Kaspersky Anti-Virus:

Ícone animado na barra de ferramentas quando executar tarefas.

Dependendo da operação que está a ser executada pela aplicação, o ícone da aplicação na bandeja do sistema altera-se. Por exemplo, se um script estiver a ser analisado, aparecerá no fundo do ícone uma pequena descrição do script, e se um e-mail estiver a ser analisado, surgirá uma imagem de uma carta. O ícone do Kaspersky Anti-Virus está animado. Neste caso, o ícone apenas irá reflectir o estado de protecção do seu computador: se a protecção estiver activada, o ícone estará a cores, e se a protecção estiver pausada ou desactivada, o ícone estará cinzento.

Activar janelas semitransparentes.

Todas as operações da aplicação que requerem a sua atenção ou decisão imediata são apresentadas como mensagens de pop-up sobre o ícone da aplicação na bandeja do sistema. As janelas da mensagem são translúcidas de forma a não interferirem com o seu trabalho. Se colocar o cursor do rato em cima da janela da mensagem, esta perde a sua transparência.

Activar notificações de notícias.

Por defeito, quando são recebidas notícias, a bandeja do sistema mostra um ícone especial, que apresenta uma janela com notícias quando clica nesse ícone.

Mostrar "Protegido pela Kaspersky Lab" no ecrã de início de sessão do Microsoft Windows.

Este indicador aparece por defeito no canto superior direito do ecrã quando o Kaspersky Anti-Virus é iniciado. Ele informa-o que o seu computador está protegido contra todos os tipos de ameaças.

> Se a aplicação estiver instalada num computador com o Microsoft Windows Vista, esta opção não estará disponível.

Para configurar elementos activos da interface, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Aparência**.
3. Na secção **Ícone da área de notificação da barra de ferramentas**, assinale ou desmarque as caixas desejadas.

MODO DE APRESENTAÇÃO DA APLICAÇÃO

Todas as cores, fontes, ícones e textos utilizados na interface do Kaspersky Anti-Virus podem ser alterados. Você pode criar os seus próprios modos de apresentação para a aplicação ou pode colocá-la numa outra linguagem.

Para usar um outro modo de apresentação da aplicação, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Aparência**.
3. Para activar um modo de apresentação, assinale a caixa **Usar modo de apresentação alternativo** na secção **Modos de apresentação**. No campo de registo, especifique a pasta com as definições do modo de apresentação. Clique no botão **Procurar** para seleccionar uma pasta.

UTILIZAR OS PERFIS DO KASPERSKY ANTI-VIRUS

A utilização de algumas aplicações (tais como, programas de jogos) em modo de ecrã inteiro pode fazer com que seja necessário desactivar determinadas funções do Kaspersky Anti-Virus, tais como o serviço de notificações. Para além disso, muitas vezes essas aplicações requerem recursos significativos do sistema, por isso a execução de determinadas tarefas do Kaspersky Anti-Virus pode conduzir ao funcionamento lento dessas aplicações.

Para evitar ter de desactivar ou pausar tarefas, manualmente, sempre que executa aplicações em ecrã inteiro, o Kaspersky Anti-Virus fornece a opção para editar temporariamente as definições, utilizando o perfil Jogos. O perfil Jogos permite editar as definições de todas as componentes em simultâneo, ao mudar para o modo de ecrã inteiro, e reverter as alterações efectuadas, ao sair desse modo.

Quando muda para o modo de ecrã inteiro, as notificações de eventos serão automaticamente desactivadas. Para além disso, pode especificar as seguintes configurações:

- **Seleccionar acção automaticamente**. Se esta configuração for seleccionada, a selecção automática da acção será aplicada a todas as componentes como uma reacção, mesmo se a opção **Perguntar o que fazer** estiver seleccionada nas respectivas configurações. Assim, o utilizador não receberá pedidos para seleccionar uma acção sobre as ameaças detectadas, uma vez que a aplicação irá seleccionar a acção automaticamente.
- **Não executar actualizações** e **Não executar tarefas de verificação agendadas**. A utilização destas configurações é recomendada para evitar que o funcionamento das aplicações de ecrã inteiro se torne lento.

Para activar o perfil Jogos, execute as seguintes acções:

1. Abra a janela principal da aplicação e clique na ligação **Configuração** na parte superior da janela.
2. Na janela que se abre, seleccione a secção **Perfil Jogos**.
3. Assinale a caixa **Activar Perfil Jogos** e especifique as configurações desejadas.

FUNCIONALIDADES ADICIONAIS

Garantir a segurança do computador é uma tarefa complexa que requer o conhecimento das funcionalidades do sistema operativo e dos métodos utilizados para explorar as suas fraquezas. Para além disso, o volume e a diversidade de informações sobre a segurança do sistema dificultam a sua análise e processamento.

Para ajudar a resolver tarefas específicas no fornecimento da segurança do computador, o pacote do Kaspersky Anti-Virus inclui um conjunto de assistentes e ferramentas:

- O Teclado Virtual (ver página 119) impede a intercepção dos dados inseridos através do teclado.
- O Assistente de Criação do Disco de Recuperação (ver página 120) restaura a funcionalidade do sistema após um ataque de vírus ou caso os ficheiros de sistema do sistema operativo fiquem corrompidos e não seja possível reiniciar o sistema tal como está.
- O Assistente de Configuração do Navegador (ver página 122) analisa as configurações do navegador Microsoft Internet Explorer, avaliando em primeiro lugar a questão da segurança.
- O Assistente de Restauro do Sistema (ver página 123) elimina os vestígios da presença de objectos de software malicioso no sistema.
- O Assistente de Limpeza de vestígio de actividade (ver página 124) procura e elimina rastreios de actividades do utilizador no sistema.

NESTA SECÇÃO:

Teclado Virtual 119

Disco de Recuperação 120

Configuração do Navegador 122

Restaurar o sistema após uma infecção 123

Assistente de Limpeza de vestígio de actividade 124

TECLADO VIRTUAL

Muitas vezes, ao trabalhar com o seu computador, é necessário inserir os seus dados pessoais ou o nome de utilizador e password. Por exemplo, quando se regista em sites da Internet ou quando utiliza lojas on-line, etc.

Existe o perigo destas informações confidenciais poderem ser interceptadas através de interceptores de teclado ou registadores de teclas digitadas (keyloggers), os quais são programas que guardam as sequências de teclas.

A ferramenta do Teclado Virtual impede a intercepção dos dados inseridos através do teclado.

O teclado virtual não consegue proteger os seus dados pessoais caso o site, que requer a inserção desses dados, tenha sido pirateado, uma vez que neste caso a informação será directamente obtida pelos intrusos.

Muitas das aplicações classificadas como spyware têm as funções de tirar fotografias do ecrã, que depois são transferidas para um intruso para análise adicional e para roubar os dados pessoais do utilizador. O teclado virtual impede que os dados pessoais inseridos sejam interceptados através da utilização de fotografias do ecrã.

O teclado virtual apenas impede a intercepção de dados de privacidade quando trabalha com os navegadores Microsoft Internet Explorer e Mozilla Firefox.

Para começar a usar o teclado virtual:

1. Abra a janela principal da aplicação.
2. Seleccione a secção **Segurança+** na parte esquerda da janela e clique no botão **Teclado virtual**.
3. Insira os dados necessários, clicando nos botões no teclado virtual. Certifique-se que os dados são inseridos no campo correcto. Quando clica nas teclas de função (**Shift**, **Alt**, **Ctrl**) no teclado virtual, esse modo particular será fixado: por exemplo, quando clica em **Shift** todos os símbolos serão inseridos em maiúsculas. Para sair do modo especial, clique novamente na mesma tecla de função.

Pode alternar o idioma do teclado virtual clicando com o botão direito do rato no botão **Shift** enquanto mantém a tecla **Ctrl** premida, ou clicando com o botão direito do rato no botão **Left Alt** enquanto mantém a tecla **Ctrl** premida, dependendo da configuração actual.

DISCO DE RECUPERAÇÃO

O Kaspersky Anti-Virus inclui um serviço que permite a criação de um disco de recuperação.

O Disco de Recuperação foi concebido para verificar e desinfectar computadores compatíveis com x86 que foram infectados. Deve ser utilizado quando a infecção atinge um nível no qual é impossível desinfectar o computador através de aplicações antivírus ou utilitários de remoção de software malicioso (tais como o Kaspersky AVPTool) em execução com o sistema operativo. Neste caso, é atingido um maior nível de eficiência na desinfecção, uma vez que os programas de software malicioso não conseguem obter controlo quando o sistema operativo está a ser carregado.

O Disco de Recuperação é um ficheiro .iso baseado no núcleo do Linux que inclui o seguinte:

- ficheiros de sistema e de configuração do Linux;
- um conjunto de utilitários de diagnóstico do sistema operativo;
- um conjunto de ferramentas adicionais (gestor de ficheiros, etc.);
- ficheiros do Kaspersky Rescue Disk;
- ficheiros que contêm bases de dados antivírus.

Um computador com o sistema operativo corrompido é iniciado a partir de um dispositivo de CD / DVD-ROM. Para o fazer, o computador deve estar equipado com um dispositivo adequado.

Para criar um disco de recuperação, execute as seguintes acções:

1. Abra a janela principal da aplicação.
2. Seleccione a secção **Segurança+** na parte esquerda da janela.
3. Clique no botão **Criar Disco de Recuperação** para executar o assistente de criação do disco.
4. Siga as instruções do assistente.
5. Através do ficheiro fornecido pelo assistente, crie um CD/DVD de arranque. Para o fazer, pode utilizar qualquer aplicação de gravação de CD / DVD, tal como o Nero.

VEJA TAMBÉM:

Criar o disco de recuperação 121

Iniciar o computador com o disco de recuperação 121

CRIAR O DISCO DE RECUPERAÇÃO

A criação de um Disco de Recuperação significa criar uma imagem do disco (ficheiro ISO) com bases de dados antivírus actualizadas e ficheiros de configuração.

A imagem de origem do disco, que serve de base à criação de um novo ficheiro, pode ser transferida a partir do servidor da Kaspersky Lab ou copiada a partir de uma origem local.

O ficheiro de imagem criado pelo assistente será guardado na pasta "*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP9\Data\Rdisk*" (ou "*ProgramData\Kaspersky Lab\AVP9\Data\Rdisk*" – para o Microsoft Vista), sendo-lhe atribuído o nome *rescuecd.iso*. Se o assistente tiver detectado um ficheiro de imagem previamente criado na pasta especificada, você pode utilizá-lo como imagem original do disco, assinalando a caixa ☑ **Utilizar um ficheiro ISO já existente** e pode saltar para o Passo 3 – Actualizar imagem. Se o assistente não detectar nenhum ficheiro de imagem, esta caixa não estará disponível.

O disco de recuperação é criado por um assistente que consiste numa série de caixas (passos), entre os quais pode navegar utilizando os botões **Anterior** e **Seguinte**; o assistente conclui o seu trabalho ao clicar no botão **Concluir**. Para parar o assistente em qualquer altura, utilize o botão **Cancelar**.

VEJA TAMBÉM:

Disco de Recuperação 120

Iniciar o computador com o disco de recuperação 121

INICIAR O COMPUTADOR COM O DISCO DE RECUPERAÇÃO

Se o sistema operativo não puder ser iniciado, como resultado de um ataque de vírus, utilize o disco de recuperação.

Irá precisar do ficheiro de imagem do disco de arranque (.iso) para carregar o sistema operativo. Pode transferir um ficheiro ISO a partir do servidor da Kaspersky Lab ou actualizar o ficheiro já existente.

Vamos analisar em maior detalhe o funcionamento do disco de recuperação. Ao carregar o disco, surgem as seguintes operações:

1. Detecção automática do hardware do computador.
2. Procura de sistemas de ficheiros em discos rígidos. Os sistemas de ficheiros detectados serão designados com nomes a começar por *C*.

   Os nomes atribuídos aos discos rígidos e dispositivos removíveis podem não corresponder aos nomes que lhes foram atribuídos pelo sistema operativo.

   Se o sistema operativo do computador que está a ser carregado estiver em modo de espera ou se o respectivo sistema de ficheiros tiver o estado *por limpar* devido a um encerramento incorrecto, você poderá escolher se deseja montar o sistema de ficheiros ou reiniciar o computador.

   A montagem do sistema de ficheiros pode resultar na sua corrupção.
3. Procura do ficheiro de comutação do Microsoft Windows *pagefile.sys*. Se este ficheiro não existir, o volume da memória virtual será limitado pelo tamanho da memória RAM.

4. Seleccionar o idioma de localização. Se a selecção não for feita após algum tempo, então o idioma Inglês será definido por defeito.

5. Procura (criação) de pastas para bases de dados antivírus, relatórios, armazenamento da quarentena e ficheiros adicionais. Por defeito, serão utilizadas as pastas das aplicações da Kaspersky Lab, instaladas no computador infectado (*ProgramData/Kaspersky Lab/AVP8* – para o Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* – para versões anteriores do Microsoft Windows). Se não for possível encontrar essas pastas de aplicações, então será feita uma tentativa para as criar. Se não for possível encontrar essas pastas e se não puderem ser criadas, será criada a pasta *kl.files* num disco do sistema.

6. Tentativa para configurar as ligações de rede, com base em dados encontrados nos ficheiros de sistema do computador que está a ser carregado.

7. Carregamento do subsistema gráfico e inicialização do Kaspersky Rescue Disk.

No modo de recuperação do sistema apenas estão disponíveis as tarefas de verificação de vírus e as actualizações da base de dados a partir de uma origem local, assim como a reversão de actualizações e a visualização de estatísticas.

➧ *Para carregar o sistema operativo de um computador infectado, execute as seguintes acções:*

1. Na configuração da BIOS, active a inicialização a partir de CD/DVD-ROM (para obter informação detalhada, por favor consulte a documentação da motherboard instalada no seu computador).

2. Insira o CD/DVD com a imagem do disco de recuperação na unidade de CD/DVD de um computador infectado.

3. Reinicie o seu computador.

O processo de inicialização continua de acordo com o algoritmo acima descrito. Para mais detalhes sobre as funcionalidades do disco de recuperação, por favor consulte a Ajuda do Kaspersky Rescue Disk.

VEJA TAMBÉM:

Disco de Recuperação 120

Criar o disco de recuperação 121

CONFIGURAÇÃO DO NAVEGADOR

O Assistente de Configuração do Navegador analisa as configurações do navegador Microsoft Internet Explorer em termos de segurança, uma vez que algumas configurações seleccionadas pelo utilizador ou predefinidas podem causar problemas de segurança.

O Assistente verifica se foram instaladas as últimas actualizações para este navegador e se as suas configurações contêm potenciais vulnerabilidades que possam ser utilizadas por intrusos para provocar danos no seu computador. Exemplos de objectos analisados:

- **Memória temporária do Microsoft Internet Explorer**. A memória temporária contém dados confidenciais, a partir dos quais também pode ser obtido um histórico dos sites visitados pelo utilizador. Alguns objectos de software malicioso também verificam a memória temporária enquanto verificam o disco e conseguem obter o endereço de e-mail do utilizador. Recomenda-se que limpe a memória temporária sempre que fechar o seu navegador.

- **Exibição de extensões para ficheiros de formatos conhecidos**. Uma opção do Windows Explorer é a ocultação de extensões de ficheiros. Muitos objectos de software malicioso utilizam uma extensão dupla, de forma a que o utilizador só consegue ver uma parte do nome do ficheiro sem a extensão real. Este esquema é muitas vezes utilizado por intrusos. Recomendamos que active a exibição de extensões para ficheiros de formatos conhecidos.

- **A lista de sites confiáveis**. Os objectos maliciosos conseguem adicionar a esta lista links para sites de intrusos.

Feche todas as janelas do Microsoft Internet Explorer antes de iniciar o diagnóstico.

Depois de a revisão estar concluída, o assistente analisa a informação para avaliar se as configurações do navegador representam problemas na segurança que requeiram atenção imediata. Este assistente irá então compilar uma lista de acções a executar para eliminar os problemas. Estas acções são agrupadas por categorias, com base na gravidade dos problemas detectados.

Quando o Assistente é concluído, será gerado um relatório, o qual pode ser enviado para a Kaspersky Lab para análise.

Note que algumas configurações podem gerar problemas com a visualização de certos sites (por exemplo, se utilizarem os controlos ActiveX). Este problema pode ser resolvido, adicionando estes sites à zona confiável.

Este assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**; para fechar o assistente depois de este concluir o seu trabalho, utilize o botão **Concluir**. Para parar o assistente em qualquer altura, utilize o botão **Cancelar**.

Para iniciar o assistente:

1. Abra a janela principal da aplicação.
2. Seleccione a secção **Segurança+** na parte esquerda da janela e clique no botão **Ajustar a Configuração do seu Navegador**.

RESTAURAR O SISTEMA APÓS UMA INFECÇÃO

O Assistente de Restauro do Sistema elimina os vestígios de acções executadas por objectos de software malicioso no sistema. A Kaspersky Lab recomenda que execute o assistente depois de o computador ter sido desinfectado, para se certificar que todas as ameaças e danos da infecção foram corrigidos. Também pode utilizar o assistente se suspeitar que o seu computador está infectado.

O assistente verifica se existem algumas alterações no sistema, tais como: o acesso à rede está bloqueado, as extensões de ficheiros de formatos conhecidos estão alteradas, a barra de ferramentas está bloqueada, etc. Esses danos podem ser causados pelas acções de programas maliciosos, falhas de sistema ou até mesmo o funcionamento incorrecto de aplicações de optimização do sistema.

Depois de a verificação estar concluída, o assistente analisa a informação para avaliar se existem danos no sistema que requeiram atenção imediata. Com base na análise, é gerada a lista de acções necessárias para eliminar os problemas. Estas acções são agrupadas por categorias, com base na gravidade dos problemas detectados.

Este assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**; para fechar o assistente depois de este concluir o seu trabalho, utilize o botão **Concluir**. Para parar o assistente em qualquer altura, utilize o botão **Cancelar**.

Para iniciar o assistente:

1. Abra a janela principal da aplicação.
2. Seleccione a secção **Segurança+** na parte esquerda da janela e clique no botão **Resolução de problemas na configuração do MS Windows**.

ASSISTENTE DE LIMPEZA DE VESTÍGIO DE ACTIVIDADE

Muitas das acções do utilizador de um computador são registadas pelo sistema: Neste caso, são guardados os seguintes dados:

- Históricos com informação sobre:
  - sites visitados;
  - inicialização de aplicações;
  - pedidos de pesquisa;
  - ficheiros abertos e guardados por diferentes aplicações.
- Registos do sistema Microsoft Windows;
- Ficheiros temporários, etc.

Todas estas fontes de informação sobre a actividade do utilizador podem conter dados confidenciais (incluindo passwords) e podem ficar disponíveis para análise pelos intrusos. Frequentemente, o utilizador não tem conhecimento suficiente para impedir o roubo de informação desta forma.

O Kaspersky Anti-Virus inclui o **Assistente de Limpeza de vestígio de actividade**. Este assistente procura rastreios de actividades do utilizador no sistema e nas configurações do sistema operativo, os quais poderiam contribuir para o armazenamento de informações sobre as actividades do utilizador.

A informação sobre as actividades do utilizador no sistema está constantemente acumulada. A inicialização de qualquer ficheiro ou a abertura de qualquer documento serão registadas. O registo do sistema Microsoft Windows regista muitos eventos ocorridos no sistema. Por esta razão, a execução repetida do **Assistente de Limpeza de vestígio de actividade** pode detectar rastreios de actividades que não foram limpos pela execução anterior do assistente. Alguns ficheiros, por exemplo o ficheiro de registo do Microsoft Windows, podem estar em uso pelo sistema enquanto o assistente está a tentar eliminá-los. Para apagar estes ficheiros, o assistente irá sugerir que você reinicie o sistema. Contudo, durante o reinício, estes ficheiros podem ser recriados e detectados novamente enquanto rastreios de actividades.

Este assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**; para fechar o assistente depois de este concluir o seu trabalho, utilize o botão **Concluir**. Para parar o assistente em qualquer altura, utilize o botão **Cancelar**.

Para iniciar o assistente:

1. Abra a janela principal da aplicação.
2. Seleccione a secção **Segurança+** na parte esquerda da janela e clique no botão **Apagar o seu Histórico de Actividades**.

RELATÓRIOS

O funcionamento de cada componente da aplicação, assim como o desempenho de cada verificação de vírus e actualização, é guardado num relatório.

Ao trabalhar com relatórios, você pode executar as seguintes acções:

- seleccionar a componente ou tarefa (ver página 126) para a qual deseja ver o relatório de eventos;
- gerir o agrupamento de dados (ver página 126) e exibir dados no ecrã (ver página 128);
- criar um agendamento (ver página 127) segundo o qual o Kaspersky Anti-Virus irá avisá-lo sobre a conclusão dos relatórios;
- seleccionar o tipo de eventos (ver página 127) sobre os quais deseja criar um relatório;
- seleccionar o modo como a informação estatística será apresentada no ecrã, sob a forma de – tabela ou gráfico (ver página 129);
- guardar o relatório em ficheiro (ver página 129);
- especificar as condições de filtragem complexa (ver página 130);
- configurar a procura de eventos (ver página 131) que ocorreram no sistema e foram processados pela aplicação.

NESTA SECÇÃO:

Seleccionar uma componente ou tarefa para criar um relatório 126

Gerir o agrupamento de informação no relatório 126

Notificação sobre a criação de relatórios 127

Seleccionar o tipo de eventos 127

Exibir Dados no Ecrã 128

Exibir estatísticas avançadas 129

Guardar o relatório num ficheiro 129

Utilizar a filtragem complexa 130

Procura de eventos 131

SELECCIONAR UMA COMPONENTE OU TAREFA PARA CRIAR UM RELATÓRIO

Você pode obter informação sobre os eventos que ocorreram durante o funcionamento de cada uma das componentes da aplicação ou durante a execução de tarefas (por exemplo, Antivírus de Ficheiros, actualização, etc.).

Para criar um relatório sobre uma determinada componente ou tarefa:

1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.
2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.
3. Na janela que se abre, na lista suspensa do lado esquerdo seleccione uma componente ou uma tarefa, para a qual deve ser criado um relatório. Quando seleccionar o item **Protecção**, será criado um relatório para todas as componentes de protecção.

GERIR O AGRUPAMENTO DE INFORMAÇÃO NO RELATÓRIO

Você pode gerir a forma como a informação é agrupada no relatório, utilizando um dos vários atributos. O conjunto de atributos difere para cada componente e tarefa da aplicação. Estão disponíveis as seguintes opções:

- **Não agrupar**. Todos os eventos serão apresentados.
- **Agrupar por tarefa**. Os dados serão agrupados de acordo com as tarefas executadas pelas componentes do Kaspersky Anti-Virus.
- **Agrupar por aplicação**. Os dados serão agrupados por aplicações que apresentem alguma actividade no sistema e serão processados pelo Kaspersky Anti-Virus.
- **Agrupar por resultado**. Os dados serão agrupados com base nos resultados da verificação ou do processamento dos objectos.

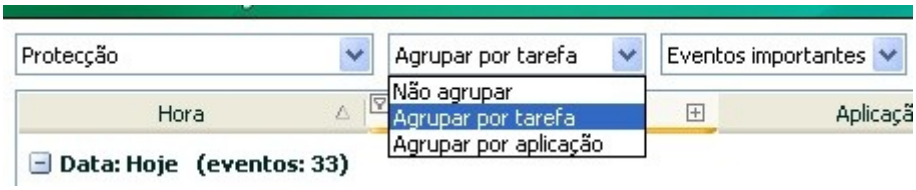


Figura 13. Atributos de agrupamento de informação no relatório

Para obter rapidamente uma informação particular e para diminuir o tamanho do agrupamento, são fornecidos critérios de pesquisa (ver secção "Procura de eventos" na página 131) por palavra-chave. Também pode especificar um critério de pesquisa.

Para agrupar a informação com base num determinado atributo:

1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.
2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.
3. Seleccione o atributo de agrupamento a partir do menu suspenso, na janela que se abre.

NOTIFICAÇÃO SOBRE A CRIAÇÃO DE RELATÓRIOS

Você pode criar um agendamento, segundo o qual o Kaspersky Anti-Virus irá avisá-lo sobre a conclusão dos relatórios.

Para criar um agendamento de notificação:

1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.
2. Na janela que se abre, no separador **Relatório**, assinale a caixa **Notificar sobre o relatório**. Clique na ligação com o valor de tempo predefinido.
3. Crie o agendamento na janela **Agendamento de relatório** que se abre.

SELECCIONAR O TIPO DE EVENTOS

A lista completa de todos os eventos ocorridos na actividade da componente de protecção, durante a execução de uma tarefa de verificação ou durante a actualização da base da dados da aplicação é registada num relatório. Você pode seleccionar os tipos de eventos que serão registados no relatório.

Os eventos podem ser atribuídos aos seguintes tipos:

- *Eventos críticos*. Eventos de importância crítica que indicam problemas no funcionamento do Kaspersky Anti-Virus ou vulnerabilidades na protecção do seu computador. Estes incluem, por exemplo, "detecção de um vírus" ou uma "falha de funcionamento"
- *Eventos importantes*. Eventos que devem ser sempre investigados, já que eles reflectem situações importantes no funcionamento da aplicação, por exemplo, evento **terminado**.

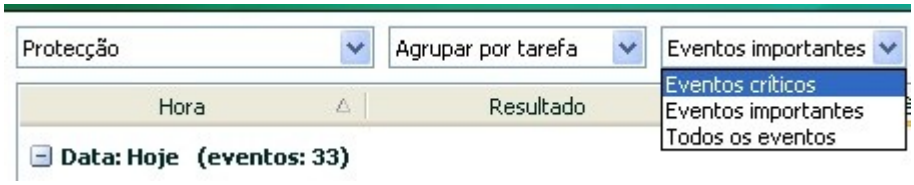


Figura 14. Seleccionar o tipo de eventos

Se o item **Todos os eventos** estiver seleccionado, serão apresentados todos os eventos no relatório, mas somente se as respectivas caixas estiverem assinaladas na área **Relatórios** da secção **Relatórios e Armazenamento** (ver secção "Registar eventos no relatório" na página 113). Estas são as caixas que permitem registar eventos não críticos, assim como eventos do sistema de ficheiros e eventos do registo, no relatório. Se estas caixas não estiverem assinaladas, serão apresentados um ícone de aviso e a ligação **Desactivado** junto à lista suspensa de selecção do tipo de eventos. Use esta ligação para aceder à janela de configuração dos relatórios e para assinalar as respectivas caixas.

Para criar um relatório sobre um determinado tipo de evento:

1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.
2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.
3. Seleccione o tipo de evento a partir do menu suspenso na janela que se abrir. Se precisar de criar um relatório sobre todos os eventos, seleccione o valor **Todos os eventos**.

EXIBIR DADOS NO ECRÃ

Os eventos incluídos no relatório serão apresentados numa tabela. Pode criar um conjunto de dados para filtrar a informação, especificando uma condição de restrição. Para o fazer, clique na área à esquerda do título da coluna da tabela para a qual deseja impor uma restrição. A lista suspensa irá apresentar os valores possíveis para as condições de restrição, por exemplo, **Ontem –** para a coluna **Hora**, **Mensagem de e-mail –** para a coluna **Objecto**, etc. Para cada coluna, seleccione o valor desejado. Pode escolher o que melhor se adequa. A consulta será executada com base na condição de restrição que especificou. Se deseja visualizar todos os dados, seleccione o item **Todos** na lista de restrições.

Figura 15. Especificar uma condição de restrição

Também pode especificar as definições de uma pesquisa complexa sob a forma de um intervalo para o qual precisa de seleccionar dados sobre eventos passados. Para o fazer, seleccione o item **Personalizar** na lista suspensa de restrições. Na janela que se abre, especifique o intervalo de tempo desejado (ver secção "Utilizar a filtragem complexa" na página 130).

Para a criar relatórios de forma fácil e simples, use o menu de atalho para aceder a qualquer atributo que permita o agrupamento e consulta de eventos.

Figura 16. Menu de contexto

- *Para especificar uma limitação:*

  1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.
  2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.
  3. Na janela que se abre, clique na área à esquerda do título da coluna da tabela para a qual deseja impor uma restrição. Seleccione a restrição desejada a partir da lista suspensa. Se seleccionar o item **Personalizar**, pode especificar condições de filtragem complexa (ver secção "Utilizar a filtragem complexa" na página 130).

- *Para ocultar/exibir colunas da tabela:*

  1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.
  2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.
  3. Na janela que se abre, clique com o botão direito do rato na área à direita do título de qualquer coluna da tabela. Para ocultar qualquer tabela da coluna, desmarque as caixas junto aos respectivos nomes no menu de contexto.

EXIBIR ESTATÍSTICAS AVANÇADAS

A parte inferior da janela de relatório contém estatísticas sobre o funcionamento da componente ou tarefa seleccionada para o Kaspersky Anti-Virus. Pode visualizar as estatísticas avançadas sob a forma de gráficos ou tabelas (com base na componente ou tarefa). Aceda às estatísticas avançadas utilizando o botão na parte superior da janela. As estatísticas são apresentadas para o dia actual e para todo o período desde o momento em que a aplicação foi instalada no seu computador.

- *Para visualizar as estatísticas avançadas, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.
  2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.
  3. Na janela que se abre, seleccione a componente da aplicação para a qual pretende visualizar as estatísticas avançadas e use o botão na parte superior da janela.

GUARDAR O RELATÓRIO NUM FICHEIRO

O relatório obtido pode ser guardado num ficheiro.

- *Para guardar o relatório obtido num ficheiro, execute as seguintes acções:*

  1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.
  2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.
  3. Na janela que se abre, crie o relatório desejado e clique no botão **Guardar**.
  4. Na janela que se abre, seleccione uma pasta na qual deseja guardar o ficheiro do relatório e insira o nome do ficheiro.

UTILIZAR A FILTRAGEM COMPLEXA

Na janela **Personalizar filtro** (ver Figura abaixo) é usada para especificar as condições de filtragem complexa dos dados. Pode usar esta janela para especificar critérios de pesquisa de dados para qualquer coluna da tabela. Vamos analisar o procedimento de trabalho com a janela, utilizando a coluna **Hora** como um exemplo.

Uma consulta de dados com um filtro complexo baseia-se na função lógica de conjunção (E lógico) e de disjunção (OU lógico) que pode ser utilizada para controlar a consulta.

Os limites da consulta (no nosso caso - Hora) estão localizados nos campos no lado direito da janela. Para especificar a hora pode utilizar as teclas de seta do seu teclado. A lista suspensa **Mostrar linhas onde:** é usada para escolher as condições da consulta de eventos (por exemplo, **é superior a**, ou seja, excede o valor especificado no campo à direita).

Figura 17. Especificar as condições de filtragem complexa

Se deseja que a sua consulta de dados satisfaça ambas as condições especificadas, seleccione **E**. Se apenas uma das duas condições precisa de ser satisfeita, seleccione **Ou**.

Para vários tipos de dados, o limite do intervalo de pesquisa não é um valor numérico ou temporal, mas sim uma palavra (por exemplo, a consulta poderia recolher o valor **OK** para a coluna **Resultado**). Neste caso, a palavra especificada como o limite será comparada com outras condições de palavra por ordem alfabética.

Para especificar as condições de filtragem complexa:

1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.

2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.

3. Na janela que se abre, clique na área à esquerda da coluna da tabela para a qual deseja especificar as condições de filtragem complexa. Seleccione o item **Personalizar** a partir do menu suspenso. Também pode seleccionar o item **Filtrar segundo este campo** a partir do menu de contexto (ver secção "Exibir dados no ecrã" na página 128) que é apresentado quando clica com o botão direito do rato na coluna da tabela desejada.

4. Na janela **Personalizar filtro** que se abre, especifique as condições de filtragem necessárias.

PROCURA DE EVENTOS

Esta janela (ver figura abaixo) foi concebida para procurar eventos que ocorreram no sistema e que foram processados pelo Kaspersky Anti-Virus.

De seguida, é apresentada a discussão dos princípios utilizados ao trabalhar com esta janela.

- O campo **Sequência** é usado para inserir a palavra-chave (por exemplo, explorer). Para iniciar a procura, clique no botão **Procurar próximo**. A procura dos dados desejados pode demorar algum tempo. Depois de a procura estar concluída, serão apresentados os eventos relacionados com a palavra-chave que inseriu. Se clicar no botão **Marcar todos** isso seleccionará todos os registos encontrados que correspondam à palavra-chave pesquisada.

- O campo **Coluna** é usado para seleccionar a coluna da tabela com base na qual será efectuada a pesquisa da palavra-chave. Esta selecção permite-lhe poupar no tempo necessário para efectuar uma pesquisa (a não ser, é claro, que não tenha seleccionado o valor **Todos**).

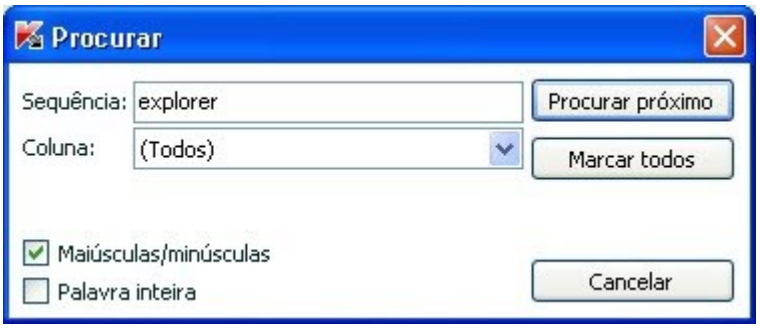


Figura 18. Procura de eventos

Para tornar a pesquisa sensível a maiúsculas/minúsculas, assinale a caixa ☑ **Maiúsculas/minúsculas**.
A caixa ☑ **Palavra inteira** irá restringir a pesquisa para que apenas se procurem palavras inteiras.

➧ *Para utilizar a procura de eventos:*

1. Abra a janela principal da aplicação e clique na ligação **Relatório** na parte superior da janela.

2. Na janela que se abre, no separador **Relatório**, clique no botão **Relatório detalhado**.

3. Na janela que se abre, clique com o botão direito do rato na área à direita do título de qualquer coluna da tabela. Seleccione o item **Procurar** a partir do menu de contexto.

4. Especifique o nome do arquivo na janela **Procurar** que se abre.

NOTIFICAÇÕES

Quando ocorrem eventos no funcionamento do Kaspersky Anti-Virus, são apresentadas mensagens especiais de notificação no ecrã. Dependendo do nível de criticalidade do evento, no que respeita à segurança do computador, você pode receber os seguintes tipos de notificações:

- **Alarme**. Ocorreu um evento crítico. Por exemplo, foi detectado um objecto de software malicioso ou uma actividade perigosa no seu sistema. Deve decidir de imediato sobre como lidar com esta ameaça. A janela deste tipo de notificação é de cor vermelha.
- **Aviso**. Ocorreu um evento potencialmente perigoso. Por exemplo, foram detectados no seu sistema ficheiros potencialmente infectados ou actividades suspeitas. Deve decidir o nível de perigo que atribui a esta acção. A janela deste tipo de notificação é de cor amarela.
- **Informação**. Esta notificação fornece-lhe informação sobre eventos que não são críticos. A janela deste tipo de notificação é de cor verde.

A janela de notificação consiste em quatro partes:

1. *Título da janela*. O título da janela de notificação contém uma breve descrição do evento. Por exemplo: pedido de direitos, actividade suspeita, nova rede, alerta, vírus.

2. *Descrição do evento*. A secção de descrição do evento apresenta informação detalhada sobre o motivo para o aparecimento da notificação: nome da aplicação que causou o evento, nome da ameaça detectada, definições da ligação de rede detectada, etc.

3. *Área de selecção da acção*. Nesta secção ser-lhe-á dada a escolha para seleccionar uma das acções disponíveis para este evento. As opções sugeridas para a acção dependem do tipo de evento, por exemplo: **Desinfectar**, **Apagar**, **Ignorar –** se tiver sido detectado um vírus, **Permitir**, **Bloquear –** no caso de um pedido por parte de uma aplicação para obter direitos para executar acções potencialmente perigosas. A acção recomendada pelos especialistas da Kaspersky Lab será apresentada a negrito.

   Se seleccionar **Permitir** ou **Bloquear**, abrir-se-á a janela onde pode seleccionar o *modo de aplicação de acções*. Para a acção **Permitir** pode seleccionar um dos seguintes modos:

   - **Permitir sempre**. Seleccione esta opção para permitir as actividades do programa, introduzindo alterações no controlo do acesso do programa aos recursos do sistema.
   - **Permitir agora**. Seleccione esta opção para aplicar a acção seleccionada a todos os eventos similares detectados durante a sessão da aplicação. A sessão da aplicação é o tempo desde o momento em que a componente foi iniciada até ao momento em que foi fechada ou reiniciada.
   - **Considerar confiável**. Seleccione esta opção para mover a aplicação para o grupo **Confiável**.

   Para a acção **Bloquear** pode seleccionar um dos seguintes modos:

   - **Bloquear sempre**. Seleccione esta opção para bloquear as actividades do programa, introduzindo alterações no controlo do acesso do programa aos recursos do sistema.
   - **Bloquear agora**. Seleccione esta opção para aplicar a acção seleccionada a todos os eventos similares detectados durante a sessão da aplicação. A sessão da aplicação é o tempo desde o momento em que a componente foi iniciada até ao momento em que foi fechada ou reiniciada.
   - **Terminar**. Seleccione esta opção para interromper a operação do programa.

4. *Área de selecção de acções adicionais*. Ao utilizar esta secção pode seleccionar uma acção adicional:

   - **Adicionar às exclusões**. Se tiver a certeza de que o objecto detectado não é malicioso, recomendamos que o adicione à zona confiável para evitar que o programa repita falsos diagnósticos positivos quando utiliza o objecto.
   - **Aplicar a todos os objectos**. Assinale esta opção para obrigar a que a acção especificada seja aplicada a todos os objectos com o mesmo estado em situações similares.

NESTA SECÇÃO:

Objecto malicioso detectado 133

Objecto não pode ser desinfectado 134

Necessidade de tratamento especial 134

Objecto perigoso detectado no tráfego 134

Objecto suspeito detectado 135

Actividade perigosa detectada no sistema 136

Processo oculto detectado 136

Detecção de tentativa de acesso ao registo do sistema 137

Ataque de phishing detectado 137

Link suspeito detectado 138

Certificado inválido detectado 138

OBJECTO MALICIOSO DETECTADO

Se o Antivírus de Ficheiros, o Antivírus de E-mail ou uma verificação de vírus detectarem um código malicioso, surgirá uma notificação especial.

A notificação conterá:

- O tipo de ameaça (por exemplo, *vírus*, *Trojan*) e o nome do objecto malicioso tal como aparece listado na Enciclopédia de Vírus da Kaspersky Lab. O nome do objecto perigoso é apresentado como um link para www.viruslist.com, onde pode encontrar informação mais detalhada sobre o tipo de ameaça detectada no seu computador.

- O nome completo do objecto malicioso e um caminho para o mesmo.

É-lhe solicitado que seleccione uma das seguintes reacções em relação ao objecto:

- **Desinfectar** – tenta desinfectar o objecto malicioso. Antes do tratamento, é efectuada uma cópia de segurança do objecto, caso surja a necessidade de o restaurar ou registar informação sobre o ficheiro que foi infectado e o programa malicioso que o infectou.

- **Apagar** – apaga o objecto malicioso. Antes de o apagar, é criada uma cópia de segurança do objecto, caso surja a necessidade de o restaurar ou registar informação sobre o ficheiro que foi infectado e o programa malicioso que o infectou.

- **Ignorar** – bloqueia o acesso ao objecto, mas não toma qualquer acção em relação ao mesmo; apenas grava a informação sobre o mesmo num relatório.

  Mais tarde, pode voltar aos objectos maliciosos ignorados na janela de relatório. Contudo, não pode adiar o processamento de objectos detectados em e-mails.

Para aplicar a acção seleccionada a todos os objectos com o mesmo estado detectados na actual sessão da componente de protecção ou tarefa, assinale a caixa ☑ **Aplicar a todos os casos semelhantes**. A actual sessão é o tempo desde que a componente é iniciada até ser desactivada ou até a aplicação ser reiniciada ou o tempo desde o início de uma verificação de vírus até à sua conclusão.

OBJECTO NÃO PODE SER DESINFECTADO

Há alguns casos em que é impossível desinfectar um objecto malicioso. Isto pode acontecer quando um objecto está tão danificado, que é impossível apagar o código malicioso do mesmo e restaurar a sua integridade. O procedimento de tratamento não pode ser aplicado a vários tipos de objectos perigosos, como por exemplo Trojans (cavalos de Tróia).

Nesses casos, surgirá uma notificação especial que contém:

- O tipo de ameaça (por exemplo, *vírus*, *Trojan*) e o nome do objecto malicioso tal como aparece listado na Enciclopédia de Vírus da Kaspersky Lab. O nome do objecto perigoso é apresentado como um link para www.viruslist.com, onde pode encontrar informação mais detalhada sobre o tipo de ameaça detectada no seu computador.

- O nome completo do objecto malicioso e um caminho para o mesmo.

É-lhe solicitado que seleccione uma das seguintes reacções em relação ao objecto:

- **Apagar** – apaga o objecto malicioso. Antes de o apagar, é criada uma cópia de segurança do objecto, caso surja a necessidade de o restaurar ou registar informação sobre o ficheiro que foi infectado e o programa malicioso que o infectou.

- **Ignorar** – bloqueia o acesso ao objecto, mas não toma qualquer acção em relação ao mesmo; apenas grava a informação sobre o mesmo num relatório.

  Mais tarde, pode voltar aos objectos maliciosos ignorados na janela de relatório. Contudo, não pode adiar o processamento de objectos detectados em e-mails.

Para aplicar a acção seleccionada a todos os objectos com o mesmo estado detectados na actual sessão da componente de protecção ou tarefa, assinale a caixa ☑ **Aplicar a todos os casos semelhantes**. A actual sessão é o tempo desde que a componente é iniciada até ser desactivada ou até a aplicação ser reiniciada ou o tempo desde o início de uma verificação de vírus até à sua conclusão.

NECESSIDADE DE TRATAMENTO ESPECIAL

Quando detecta uma ameaça que está actualmente activa no sistema (por exemplo, é detectado um processo malicioso na sua RAM ou em objectos de inicialização), aparecerá uma mensagem a sugerir-lhe que execute um procedimento especial de desinfecção avançada.

Os especialistas da Kaspersky Lab recomendam vivamente que concorde com a execução do procedimento de desinfecção avançada. Para o fazer, clique no botão **OK**. Contudo, tenha em atenção que o computador reiniciar-se-á depois de concluir este procedimento, por isso recomendamos que guarde o seu actual trabalho e feche todas as aplicações antes de executar o procedimento.

Enquanto procedimento de desinfecção estiver a decorrer, não poderá iniciar o cliente de e-mail ou editar o registo do sistema operativo. Depois de reiniciar o computador, recomendamos que execute a verificação completa de vírus.

OBJECTO PERIGOSO DETECTADO NO TRÁFEGO

Quando o Antivírus de Internet detecta um objecto malicioso no tráfego, surge uma notificação especial no ecrã.

A notificação contém:

- O tipo de ameaça (por exemplo, *variante de vírus*) e o nome do objecto perigoso tal como aparece listado na Enciclopédia de Vírus da Kaspersky Lab. O nome do objecto é apresentado como um link para www.viruslist.com, onde pode encontrar informação mais detalhada sobre o tipo de ameaça detectada.

- O nome completo do objecto malicioso e um caminho para a página de Internet.

É-lhe solicitado que seleccione uma das seguintes reacções em relação ao objecto:

- **Permitir** – continua a transferência do objecto.
- **Bloquear** – bloqueia a transferência do objecto a partir da recurso de Internet.

Para aplicar a acção seleccionada a todos os objectos com o mesmo estado detectados na actual sessão da componente de protecção ou tarefa, assinale a caixa ☑ **Aplicar a todos os casos semelhantes**. A actual sessão é o tempo desde que a componente é iniciada até ser desactivada ou até a aplicação ser reiniciada ou o tempo desde o início de uma verificação de vírus até à sua conclusão.

OBJECTO SUSPEITO DETECTADO

Se o Antivírus de Ficheiros, o Antivírus de E-mail ou uma verificação de vírus detectarem um objecto que contém código de um vírus desconhecido ou código modificado de um vírus conhecido, surgirá uma notificação especial.

A notificação conterá:

- O tipo de ameaça (por exemplo, *vírus*, *Trojan*) e o nome do objecto tal como aparece listado na Enciclopédia de Vírus da Kaspersky Lab. O nome do objecto perigoso é apresentado como um link para www.viruslist.com, onde pode encontrar informação mais detalhada sobre o tipo de ameaça detectada no seu computador.
- O nome completo do objecto e um caminho para o mesmo.

É-lhe solicitado que seleccione uma das seguintes reacções em relação ao objecto:

- **Quarentena** – move o objecto para a quarentena. Quando coloca um objecto em Quarentena, esse objecto não é copiado, mas sim movido: o objecto é apagado do disco ou e-mail e é guardado na pasta da Quarentena. Os ficheiros em Quarentena são guardados num formato especial e não são perigosos.

  Mais tarde, quando verifica a Quarentena com assinaturas de ameaças actualizadas, o estado do objecto pode alterar-se. Por exemplo, o objecto pode ser identificado como infectado e pode ser processado, utilizando uma base de dados actualizada. Por outro lado, poderia ser atribuído o estado *não infectado* ao objecto e depois poderia ser restaurado.

  Se um ficheiro for, manualmente, colocado na quarentena e se, depois de uma verificação subsequente, se conclui que o objecto não está infectado, o seu estado após a verificação não, será automaticamente, alterado para *OK*. Isto apenas acontecerá se a verificação ocorrer decorrido um certo tempo (pelo menos, três dias) após a sua colocação na quarentena.

- **Apagar** – apaga o objecto. Antes de o apagar, é criada uma cópia de segurança do objecto, caso surja a necessidade de o restaurar ou registar informação sobre o ficheiro que foi infectado e o programa malicioso que o infectou.
- **Ignorar** – bloqueia o acesso ao objecto, mas não toma qualquer acção em relação ao mesmo; apenas grava a informação sobre o mesmo num relatório.

  Mais tarde, pode voltar aos objectos ignorados na janela de relatório. Contudo, não pode adiar o processamento de objectos detectados em e-mails.

Para aplicar a acção seleccionada a todos os objectos com o mesmo estado detectados na actual sessão da componente de protecção ou tarefa, assinale a caixa ☑ **Aplicar a todos os casos semelhantes**. A actual sessão é o tempo desde que a componente é iniciada até ser desactivada ou até a aplicação ser reiniciada ou o tempo desde o início de uma verificação de vírus até à sua conclusão.

Se tiver a certeza de que o objecto detectado não é malicioso, recomendamos que o adicione à zona confiável para evitar que o programa repita falsos diagnósticos positivos quando utiliza o objecto.

ACTIVIDADE PERIGOSA DETECTADA NO SISTEMA

Quando a Defesa Proactiva detecta uma actividade perigosa de uma aplicação do seu sistema, surge uma notificação especial que contém:

- O nome da ameaça, tal como aparece listada na Enciclopédia de Vírus da Kaspersky Lab. O nome da ameaça é apresentado como um link para www.viruslist.com, onde pode encontrar informação mais detalhada sobre o tipo de ameaça detectada.
- O nome completo do ficheiro do processo que iniciou a actividade perigosa e um caminho para o ficheiro.
- As reacções possíveis:
  - **Quarentena** – fecha o processo e coloca o ficheiro executável em quarentena. Quando coloca um objecto em Quarentena, esse objecto não é copiado, mas sim movido. Os ficheiros em Quarentena são guardados num formato especial e não são perigosos.

    Mais tarde, quando verifica a Quarentena com assinaturas de ameaças actualizadas, o estado do objecto pode alterar-se. Por exemplo, o objecto pode ser identificado como infectado e pode ser processado, utilizando uma base de dados actualizada. Por outro lado, poderia ser atribuído o estado *não infectado* ao objecto e depois poderia ser restaurado.

    Se um ficheiro for, manualmente, colocado na quarentena e se, depois de uma verificação subsequente, se conclui que o objecto não está infectado, o seu estado após a verificação não, será automaticamente, alterado para *OK*. Isto apenas acontecerá se a verificação ocorrer decorrido um certo tempo (pelo menos, três dias) após a sua colocação na quarentena.
  - **Terminar** – encerra o processo.
  - **Permitir** – permite que o processo seja executado.

Para aplicar a acção seleccionada a todos os objectos com o mesmo estado detectados na actual sessão da componente de protecção ou tarefa, assinale a caixa ☑ **Aplicar a todos os casos semelhantes**. A actual sessão é o tempo desde que a componente é iniciada até ser desactivada ou até a aplicação ser reiniciada ou o tempo desde o início de uma verificação de vírus até à sua conclusão.

Se tiver a certeza de que o programa detectado não é perigoso, recomendamos que o adicione à zona confiável para evitar que o Kaspersky Anti-Virus repita falsos diagnósticos positivos quando o detectar.

PROCESSO OCULTO DETECTADO

Quando a Defesa Proactiva detecta um processo oculto no seu sistema, surge uma notificação especial que contém:

- O nome da ameaça, tal como aparece listada na Enciclopédia de Vírus da Kaspersky Lab. O nome da ameaça é apresentado como um link para www.viruslist.com, onde pode encontrar informação mais detalhada sobre o tipo de ameaça detectada.
- O nome completo do ficheiro do processo oculto e um caminho para o ficheiro.
- As reacções possíveis:
  - **Quarentena** – move o ficheiro executável do processo para a quarentena. Quando coloca um objecto em Quarentena, esse objecto não é copiado, mas sim movido. Os ficheiros em Quarentena são guardados num formato especial e não são perigosos.

    Mais tarde, quando verifica a Quarentena com assinaturas de ameaças actualizadas, o estado do objecto pode alterar-se. Por exemplo, o objecto pode ser identificado como infectado e pode ser processado, utilizando uma base de dados actualizada. Por outro lado, poderia ser atribuído o estado *não infectado* ao objecto e depois poderia ser restaurado.

Se um ficheiro for, manualmente, colocado na quarentena e se, depois de uma verificação subsequente, se conclui que o objecto não está infectado, o seu estado após a verificação não, será automaticamente, alterado para *OK*. Isto apenas acontecerá se a verificação ocorrer decorrido um certo tempo (pelo menos, três dias) após a sua colocação na quarentena.

- **Terminar** – encerra o processo.
- **Permitir** – permite que o processo seja executado.

Para aplicar a acção seleccionada a todos os objectos com o mesmo estado detectados na actual sessão da componente de protecção ou tarefa, assinale a caixa ☑ **Aplicar a todos os casos semelhantes**. A actual sessão é o tempo desde que a componente é iniciada até ser desactivada ou até a aplicação ser reiniciada ou o tempo desde o início de uma verificação de vírus até à sua conclusão.

Se tiver a certeza de que o programa detectado não é perigoso, recomendamos que o adicione à zona confiável para evitar que o Kaspersky Anti-Virus repita falsos diagnósticos positivos quando o detectar.

DETECÇÃO DE TENTATIVA DE ACESSO AO REGISTO DO SISTEMA

Quando a Defesa Proactiva detecta uma tentativa de acesso às chaves de registo do sistema, surge uma notificação especial que contém:

- A chave de registo que está a ser acedida.
- O nome completo do ficheiro do processo que iniciou a tentativa de acesso às chaves de registo e um caminho para o ficheiro.
- As reacções possíveis:
  - **Permitir** – permite que a acção perigosa seja executada uma vez;
  - **Bloquear** – bloqueia a acção perigosa uma vez.

Para executar a acção que você seleccionar, automaticamente, todas as vezes que esta actividade for iniciada no seu computador, assinale a caixa ☑ **Criar uma regra**.

Se tiver a certeza de que qualquer actividade da aplicação que tentou aceder às chaves de registo do sistema não é perigosa, adicione a aplicação à lista de aplicações confiáveis.

ATAQUE DE PHISHING DETECTADO

Sempre que o Kaspersky Anti-Virus detecta um ataque de phishing (pesca ilegal de informação), surgirá uma notificação especial.

A notificação conterá:

- O nome da ameaça (*ataque de phishing*) sendo apresentado como um link para a Enciclopédia de Vírus da Kaspersky Lab, com uma descrição detalhada da ameaça.
- O endereço da Internet para o ataque de phishing.
- As reacções possíveis:
  - **Permitir** – continua a transferência do site de phishing.
  - **Bloquear** – bloqueia a transferência do site de phishing.

Para aplicar a acção seleccionada a todos os objectos com o mesmo estado detectados na actual sessão da componente de protecção ou tarefa, assinale a caixa **Aplicar a todos os casos semelhantes**. A actual sessão é o tempo desde que a componente é iniciada até ser desactivada ou até a aplicação ser reiniciada ou o tempo desde o início de uma verificação de vírus até à sua conclusão.

LINK SUSPEITO DETECTADO

Sempre que o Kaspersky Anti-Virus detecta uma tentativa para abrir um site, cujo endereço está contido na lista de endereços de Internet suspeitos, surgirá uma notificação especial.

A notificação conterá:

- O endereço do site.
- As reacções possíveis:
  - **Permitir** – continua a transferência do site.
  - **Bloquear** – bloqueia a transferência do site.

Para aplicar a acção seleccionada a todos os objectos com o mesmo estado detectados na actual sessão da componente de protecção ou tarefa, assinale a caixa **Aplicar a todos os casos semelhantes**. A actual sessão é o tempo desde que a componente é iniciada até ser desactivada ou até a aplicação ser reiniciada ou o tempo desde o início de uma verificação de vírus até à sua conclusão.

CERTIFICADO INVÁLIDO DETECTADO

A verificação de segurança para a ligação através do protocolo SSL é executada utilizando o certificado instalado. Se for detectado um certificado inválido quando for tentada a ligação ao servidor (por exemplo, se o certificado for substituído por um intruso), será apresentada uma notificação no ecrã.

A notificação conterá informação sobre a possível causa de erro e identificará a porta e o endereço remotos. Ser-lhe-á pedido que decida se se deverá continuar a ligação com um certificado inválido:

- **Aceitar certificado** – continuar a ligação ao site;
- **Recusar certificado** – interromper a ligação ao site;
- **Ver certificado** – ver informação sobre o certificado.

VALIDAR A CONFIGURAÇÃO DO KASPERSKY ANTI-VIRUS

Depois de instalar e configurar o Kaspersky Anti-Virus, pode verificar se a aplicação está correctamente configurada, usando um "vírus" de teste e variantes do mesmo. É necessário um teste separado para cada componente de protecção / protocolo.

NESTA SECÇÃO:

Testar o "vírus" EICAR e suas variantes 139

Testar a protecção do tráfego de HTTP 140

Testar a protecção do tráfego de SMTP 141

Validar a configuração do Antivírus de Ficheiros 141

Validar a configuração das tarefas de verificação de vírus 141

TESTAR O "VÍRUS" EICAR E SUAS VARIANTES

Este "vírus" de teste foi, especialmente, desenvolvido pelo eicar (O Instituto Europeu para Pesquisa de Antivírus de Computador) para testar os produtos antivírus.

O "vírus" de teste NÃO É UM VÍRUS porque não contém código que possa danificar o seu computador. Contudo, a maioria dos produtos antivírus identifica este ficheiro como um vírus.

Nunca use vírus reais para testar o funcionamento de um produto antivírus!

Tente transferir um "vírus" de teste a partir do site oficial do **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

Antes de transferir o ficheiro, tem de desactivar a protecção antivírus, caso contrário a aplicação iria identificar e processar o ficheiro *anti_virus_test_file.htm* como um objecto infectado transferido através do protocolo HTTP. Não se esqueça de activar a protecção antivírus imediatamente depois de transferir o "vírus" de teste.

A aplicação identifica o ficheiro transferido do site do **EICAR** como um objecto infectado que contém um vírus que **não pode ser desinfectado** e executa as acções especificadas para este tipo de objecto.

Também pode alterar o "vírus" de teste padrão para verificar o funcionamento da aplicação. Para alterar o "vírus", altere os conteúdos do "vírus" padrão, adicionando-lhe um dos prefixos (ver tabela que se segue). Para alterar o "vírus" de teste, pode utilizar qualquer editor de texto ou hipertexto, como por exemplo o **Microsoft Notepad**, **UltraEdit32**, etc.

Só pode testar a adequação do funcionamento da aplicação antivírus (através do "vírus" alterado do EICAR) caso as suas bases antivírus tenham sido actualizadas em ou depois de 24 de Outubro de 2003 (actualizações acumuladas de Outubro, 2003).

Na tabela que se segue, a primeira coluna contém os prefixos que é necessário adicionar ao início do "vírus" de teste padrão. A segunda coluna lista os possíveis estados que a aplicação Antivírus pode atribuir ao objecto, com base nos resultados da verificação. A terceira coluna indica a forma como a aplicação processa os objectos com o estado especificado. Por favor, note que as acções efectivamente executadas sobre os objectos são determinadas pelas configurações da aplicação.

Depois de adicionar o prefixo ao "vírus" de teste, guarde o novo ficheiro com um nome diferente, por exemplo: *eicar_dele.com*. Atribua nomes similares a todos os "vírus" alterados.

Table 1. Alterações do "vírus" de teste

Prefixo	Estado do objecto	Informação de processamento do objecto
Sem prefixo, "vírus" de teste padrão	**Infectado**. O objecto contém código de um vírus conhecido. Você não pode desinfectar o objecto.	A aplicação identifica o objecto como um vírus não desinfectável. Ocorre um erro ao tentar desinfectar o objecto; a acção executada será a especificada para objectos não desinfectáveis.
CORR-	**Corrompido**.	A aplicação conseguia aceder ao objecto, mas não conseguiu verificá-lo, uma vez que o objecto está corrompido (por exemplo, a estrutura de ficheiro está corrompida ou o formato de ficheiro é inválido). Pode encontrar informação sobre a forma como o objecto foi processado no relatório de funcionamento da aplicação.
WARN-	**Suspeito**. O objecto contém código de um vírus desconhecido. Você não pode desinfectar o objecto.	O objecto foi considerado suspeito pelo analisador de código heurístico. Na altura da detecção, as bases de dados antivírus de assinaturas de ameaças não contêm uma descrição do procedimento para tratar este objecto. Você será notificado quando um objecto deste tipo for detectado.
SUSP-	**Suspeito**. O objecto contém código alterado de um vírus conhecido. Você não pode desinfectar o objecto.	A aplicação detectou uma correspondência parcial entre uma secção do código do objecto e uma secção de código de um vírus conhecido. Na altura da detecção, as bases de dados antivírus de assinaturas de ameaças não contêm uma descrição do procedimento para tratar este objecto. Você será notificado quando um objecto deste tipo for detectado.
ERRO-	**Erro de verificação**.	Ocorreu um erro durante a verificação de um objecto. A aplicação não conseguiu aceder ao objecto, uma vez que a integridade do objecto foi violada (por exemplo, não há fim para um arquivo multi-volume) ou não existe ligação para o mesmo (se o objecto é verificado num recurso de rede). Pode encontrar informação sobre a forma como o objecto foi processado no relatório de funcionamento da aplicação.
CURE-	**Infectado**. O objecto contém código de um vírus conhecido. Desinfectável.	O objecto contém um vírus que pode ser desinfectado. A aplicação irá desinfectar o objecto; o texto do corpo do "vírus" será substituído pela palavra CURE. Você será notificado quando um objecto deste tipo for detectado.
DELE-	**Infectado**. O objecto contém código de um vírus conhecido. Você não pode desinfectar o objecto.	A aplicação identifica o objecto como um vírus não desinfectável. Ocorre um erro ao tentar desinfectar o objecto; a acção executada será a especificada para objectos não desinfectáveis. Você será notificado quando um objecto deste tipo for detectado.

TESTAR A PROTECÇÃO DO TRÁFEGO DE HTTP

- *Para verificar que os vírus são detectados com sucesso em fluxos de dados transferidos através do protocolo HTTP, execute as seguintes acções:*

  tente transferir um "vírus" de teste a partir do site oficial do **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

Quando o computador tenta transferir o "vírus" de teste, o Kaspersky Anti-Virus irá detectar o objecto, identificá-lo como um objecto infectado que não pode ser desinfectado e irá executar a acção especificada nas configurações de verificação do tráfego HTTP para objectos com este estado. Por defeito, quando tenta transferir o "vírus" de teste, a ligação com o site será terminada e o navegador irá apresentar uma mensagem a indicar que este objecto está infectado com o vírus EICAR-Test-File.

TESTAR A PROTECÇÃO DO TRÁFEGO DE SMTP

Para detectar vírus em fluxos de dados transferidos através do protocolo SMTP, tem de usar um sistema de e-mail que utiliza este protocolo para transferir dados.

Recomendamos que teste a forma como o Antivírus processa os e-mails enviados, incluindo quer o corpo da mensagem, quer os anexos. Para testar a detecção de vírus no corpo da mensagem, copie o texto do "vírus" de teste padrão ou do "vírus" alterado para o corpo da mensagem.

Para o fazer:

1. Crie uma mensagem de formato **Texto simples**, utilizando um cliente de e-mail instalado no seu computador.

   Uma mensagem que contenha um vírus de teste não será verificada se for criada em formato RTF ou HTML!

2. Copie o texto do "vírus" padrão ou alterado no início da mensagem ou anexe um ficheiro com o "vírus" de teste à mensagem.
3. Envie a mensagem para o administrador.

A aplicação deverá detectar o objecto, identificá-lo como infectado e bloquear a mensagem.

VALIDAR A CONFIGURAÇÃO DO ANTIVÍRUS DE FICHEIROS

Para verificar se o Antivírus de Ficheiros está correctamente configurado:

1. Crie uma pasta no disco. Copie para essa pasta o "vírus" de teste que transferiu a partir do site oficial do **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), assim como todos os "vírus" de teste alterados que criou.
2. Permita que todos os eventos sejam registados, para que o ficheiro de relatório retenha dados sobre objectos corrompidos ou objectos ignorados devido a erros.
3. Execute o "vírus" de teste ou uma das suas versões alteradas.

O Antivírus de Ficheiros irá interceptar a chamada para executar o ficheiro, irá verificá-lo e irá executar a acção especificada nas configurações para objectos com esse estado. Ao seleccionar diferentes acções a executar sobre o objecto detectado, pode executar uma verificação completa do funcionamento da componente.

Pode ver informação sobre os resultados do funcionamento do Antivírus de Ficheiros no relatório de funcionamento da componente.

VALIDAR A CONFIGURAÇÃO DAS TAREFAS DE VERIFICAÇÃO DE VÍRUS

Para verificar se a tarefa de verificação de vírus está correctamente configurada:

1. Crie uma pasta no disco. Copie para essa pasta o "vírus" de teste que transferiu a partir do site oficial do **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), assim como todos os "vírus" de teste alterados que criou.
2. Crie uma nova tarefa de verificação de vírus e seleccione a pasta que contém o conjunto de "vírus" de teste como o objecto a verificar.
3. Permita que todos os eventos sejam registados, para que o ficheiro de relatório retenha dados sobre objectos corrompidos e objectos não verificados devido a erros.
4. Execute a tarefa de verificação de vírus.

Quando a tarefa de verificação estiver em execução, as acções especificadas na configuração da tarefa serão executadas à medida que forem detectados objectos suspeitos ou infectados. Ao seleccionar diferentes acções a executar sobre o objecto detectado, pode executar uma verificação completa do funcionamento da componente.

Pode ver informação completa sobre as acções da tarefa de verificação de vírus no relatório de funcionamento da componente.

TRABALHAR COM A APLICAÇÃO A PARTIR DA LINHA DE COMANDOS

Você pode trabalhar com o Kaspersky Anti-Virus a partir da linha de comandos. Pode executar as seguintes operações:

- iniciar e parar as componentes da aplicação;
- iniciar e parar as tarefas de verificações de vírus;
- obter informação sobre o estado actual das componentes, tarefas e suas estatísticas;
- verificar objectos seleccionados;
- actualizar bases de dados e módulos da aplicação;
- aceder à Ajuda para a sintaxe de acção do comando;
- aceder à Ajuda para a sintaxe do comando.

Sintaxe de acção do comando:

```
avp.com <comando> [opções]
```

Tem que aceder à aplicação através da linha de comandos a partir da pasta de instalação da aplicação ou especificando o caminho completo para avp.com.

São fornecidos os seguintes comandos:

START	Inicia uma componente ou tarefa.
STOP	Pára uma componente ou tarefa. O comando só podem ser executado se for inserida a password atribuída através da interface do Kaspersky Anti-Virus.
STATUS	Mostra o estado da componente ou tarefa actual no ecrã.
STATISTICS	Mostra as estatísticas para a componente ou tarefa no ecrã.
HELP	Ajuda com a sintaxe do comando e a lista de comandos.
SCAN	Verifica objectos em termos de vírus.
UPDATE	Inicia a actualização da aplicação
ROLLBACK	Reverte para a última actualização do Kaspersky Anti-Virus. O comando só podem ser executado se for inserida a password atribuída através da interface da aplicação.
EXIT	Fecha a aplicação. O comando só podem ser executado se for inserida a password atribuída através da interface da aplicação.

IMPORT	Importa as definições de protecção da aplicação. O comando só podem ser executado se for inserida a password atribuída através da interface do Kaspersky Anti-Virus.
EXPORT	Exporta as definições de protecção da aplicação.

Cada comando requer o seu próprio conjunto específico de parâmetros.

NESTA SECÇÃO:

Gerir componentes e tarefas da aplicação 143

Verificação de vírus 145

Actualizar a aplicação 148

Reverter a última actualização 149

Exportar as definições de protecção 149

Importar as definições de protecção 150

Iniciar a aplicação 150

Parar a aplicação 150

Criar um ficheiro de rastreio 150

Visualizar a Ajuda 151

Códigos de retorno da interface da linha de comandos 151

GERIR COMPONENTES E TAREFAS DA APLICAÇÃO

Sintaxe do comando:

```
avp.com <comando> <perfil|nome_tarefa> [/R[A]:<ficheiro_relatório>]
avp.com STOP|PAUSE <perfil|nome_tarefa> /password=<sua_password>
[/R[A]:<ficheiro_relatório>]
```

<comando>	Você pode gerir as componentes e tarefas do Kaspersky Anti-Virus a partir do comando de acção com os seguintes comandos: START – iniciar uma componente ou tarefa de protecção. STOP – parar uma componente ou tarefa de protecção. STATUS – apresenta o actual estado de uma componente ou tarefa de protecção. STATISTICS – apresenta estatísticas no ecrã para uma componente ou tarefa de protecção. Note que não pode executar o comando STOP sem introduzir a password.

<perfil|nome_tarefa>	Pode especificar qualquer componente de protecção do Kaspersky Anti-Virus, módulo das componentes, tarefa de verificação sob pedido ou de actualização para os valores da configuração **<perfil>** (os valores padrão utilizados pela aplicação são apresentados na tabela abaixo). Pode especificar o nome de qualquer tarefa de verificação sob pedido ou de actualização como o valor para a configuração **<nome_tarefa>**.
<sua_password>	A password da aplicação especificada na interface.
/R[A]:<ficheiro_relatório>	**/R:<ficheiro_relatório>** – apenas regista eventos importantes no relatório. **/RA:<ficheiro_relatório>** – regista todos os eventos no relatório. Pode usar um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.

A configuração **<perfil>** pode ter um dos seguintes valores:

RTP	Todas as componentes de protecção. O comando **avp.com START RTP** inicia todas as todas as componentes de protecção, se a protecção estiver desactivada por completo. Se a componente foi desactivada com o comando **STOP** a partir da linha de comandos, o comando **avp.com START RTP** não irá iniciá-la. Para a iniciar, tem que executar o comando **avp.com START <perfil>**, com o nome da componente de protecção específica inserido para **<perfil>**. Por exemplo, **avp.com START FM**.
pdm	Defesa Proactiva
FM	Antivírus de Ficheiros
EM	Antivírus de E-mail
WM	Antivírus de Internet Valores para as subcomponentes do Antivírus de Internet: **httpscan (HTTP)** – verifica tráfego de HTTP; **sc** – verifica scripts.
IM	Antivírus de MI
Updater	Actualização
Rollback	Reverter a última actualização
Scan_My_Computer	Verificação do computador
Scan_Objects	Verificação de Objectos
Scan_Quarantine	Verificação da Quarentena

Scan_Rootkits	Verificação de processos ocultos
Scan_Startup (STARTUP)	Verificação de objectos de inicialização
Scan_Vulnerabilities (SECURITY)	Verificação de vulnerabilidades

As componentes e tarefas iniciadas a partir do comando de acção são executadas com as definições configuradas na interface da aplicação.

Exemplos:

- *Para activar o Antivírus de Ficheiros, digite isto na linha de comandos:*

  ```
  avp.com START FM
  ```

- *Para retomar o Controlo Parental, digite isto na linha de comandos:*

  ```
  avp.com RESUME ParCtl
  ```

- *Para parar uma tarefa de verificação do computador a partir da linha de comandos, introduza:*

  ```
  avp.com STOP Scan_My_Computer /password=<sua_password>
  ```

VERIFICAÇÃO DE VÍRUS

Iniciar uma verificação de vírus de determinada área e processar objectos maliciosos a partir de um comando de acção tem, geralmente, o seguinte aspecto:

```
avp.com SCAN [<objecto verificado>] [<acção>] [<tipos de ficheiro>] [<exclusões>]
[<ficheiro de configuração>] [<configurações de relatórios>] [<configurações
avançadas>]
```

Para analisar objectos, você também pode usar as tarefas criadas na aplicação, iniciando a tarefa que precisa a partir da linha de comandos. A tarefa será executada com as definições especificadas na interface do Kaspersky Anti-Virus.

Descrição das definições:

<objecto a verificar> – este parâmetro dá-lhe a lista de objectos que serão analisados em termos de código malicioso. O parâmetro pode incluir vários valores da lista fornecida, separados por espaços.	
<ficheiros>	Lista de caminhos para os ficheiros e/ou pastas a serem analisados. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Os itens da lista estão separados por um espaço. Comentários: • se o nome do objecto tiver um espaço, deve ser colocado entre aspas; • se for feita referência a uma pasta específica, todos os ficheiros existentes na mesma serão analisados.
/MEMORY	Objectos da memória RAM.
/STARTUP	Objectos de inicialização.

/MAIL	Caixas de e-mail.
/REMDRIVES	Todos os discos removíveis.
/FIXDRIVES	Todos os discos internos.
/NETDRIVES	Todos os discos de rede.
/QUARANTINE	Objectos em quarentena.
/ALL	Verificação completa do computador.
/@:<filelist.lst>	Caminho para um ficheiro com uma lista de objectos e pastas a serem verificados. O ficheiro deve estar em formato texto e cada objecto de verificação deve estar listado numa linha separada. Pode introduzir um caminho absoluto ou relativo para o ficheiro. O caminho deve ser colocado entre aspas se tiver um espaço.
<acção> – este parâmetro determina a acção que será tomada com os objectos maliciosos detectados durante a verificação. Se este parâmetro não for definido, a acção predefinida é aquela com o valor para **/i8.** Se estiver a trabalhar em modo automático, o Kaspersky Anti-Virus aplicará automaticamente a acção recomendada pelos especialistas da Kaspersky Lab quando forem detectados objectos perigosos. Uma acção que corresponde ao valor do parâmetro **<acção>** será ignorada.	
/i0	Não actua sobre o objecto; simplesmente guarda informação sobre o mesmo no relatório.
/i1	Trata objectos infectados e, se a desinfecção for impossível, ignora-os.
/i2	Trata objectos infectados e, se a desinfecção falhar, apaga-os. Não apaga objectos infectados de objectos compostos. Apaga objectos compostos com cabeçalhos executáveis (arquivos sfx) (esta é a predefinição).
/i3	Trata objectos infectados e, se a desinfecção falhar, apaga-os. Apaga completamente todos os objectos compostos se as partes infectadas não puderem ser apagadas.
/i4	Apaga objectos infectados. Apaga completamente todos os objectos compostos se as partes infectadas não puderem ser apagadas.
/i8	Perguntar ao utilizador a acção a efectuar se for detectado um objecto infectado.
/i9	Perguntar ao utilizador a acção a efectuar no final da verificação.
<tipos de ficheiro> – este parâmetro define os tipos de ficheiros que serão sujeitos à verificação do antivírus. Por defeito, se este parâmetro não for definido, apenas serão verificados os ficheiros infectados por conteúdo.	
/fe	Verifica por extensão só os ficheiros infectados.
/fi	Verifica por conteúdo só os ficheiros infectados.
/fa	Verifica todos os ficheiros.
<exclusões> – este parâmetro define os objectos excluídos da verificação. O parâmetro pode incluir vários valores da lista fornecida, separados por espaços.	
-e:a	Não verifica arquivos.

-e:b	Não verifica bases de dados de e-mail.
-e:m	Não verifica e-mail com texto simples.
-e:<máscara de ficheiro>	Não verifica objectos que correspondam à máscara.
-e:<segundos>	Ignora os objectos que são verificados durante um tempo superior àquele especificado no parâmetro **<segundos>**.
-es:<tamanho>	Ignora objectos com tamanho superior (em MB) ao valor especificado no parâmetro **<tamanho>**.
<ficheiro de configuração> – define o caminho para o ficheiro de configuração que contém as definições da aplicação para a verificação. O ficheiro de configuração é um ficheiro em formato de texto que contém o conjunto dos parâmetros da linha de comandos para a verificação antivírus. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, são utilizados os valores definidos na interface da aplicação.	
/C:<nome_ficheiro>	Utiliza os valores das definições especificados no ficheiro de configuração **<nome_ficheiro>**.
<configurações de relatórios> – este parâmetro determina o formato do relatório dos resultados da verificação. Pode usar um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.	
/R:<ficheiro_relatório>	Só regista eventos importantes neste ficheiro.
/RA:<ficheiro_relatório>	Regista todos os eventos neste ficheiro.
<configurações avançadas> – definições que determinam a utilização das tecnologias de verificação antivírus.	
/iChecker=<on|off>	Activar/ desactivar a utilização da tecnologia iChecker.
/iSwift=<on|off>	Activar/ desactivar a utilização da tecnologia iSwift.

Exemplos:

- *Iniciar uma verificação da memória, Programas de Inicialização, caixas de e-mail, os directórios Os Meus Documentos e Ficheiros de Programa e o ficheiro test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

- *Pausar a verificação dos objectos seleccionados e iniciar a verificação completa do computador e depois de esta continuar com a verificação pausada:*

```
avp.com PAUSE Scan_Objects /password=<sua_password>
avp.com START Scan_My_Computer
avp.com RESUME Scan_Objects
```

- *Analisar os objectos listados no ficheiro object2scan.txt, utilizando o ficheiro de configuração scan_setting.txt. Utilizar o ficheiro de configuração scan_setting.txt. Quanto a verificação estiver concluída, criar um relatório para registar todos os eventos:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Uma amostra de um ficheiro de configuração:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

ACTUALIZAR A APLICAÇÃO

A sintaxe para actualizar os módulos do Kaspersky Anti-Virus e as bases de dados da aplicação a partir do comando de acção é a seguinte:

```
avp.com UPDATE [<origem_actualização>] [/R[A]:<ficheiro_relatório>]
[/C:<nome_ficheiro>] [/APP=<on|off>]
```

Descrição das definições:

<origem_actualização>	Servidor HTTP ou FTP ou pasta da rede para transferir actualizações. O valor para este parâmetro pode ser especificado sob a forma de um caminho completo para uma origem de actualização ou um URL. Se não for seleccionado um caminho, a origem de actualização será tirada das definições de actualização da aplicação.
/R[A]:<ficheiro_relatório>	**/R:**<ficheiro_relatório> – apenas regista eventos importantes no relatório. **/RA:**<ficheiro_relatório> – regista todos os eventos no relatório. Pode usar um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.
/C:<nome_ficheiro>	Caminho para o ficheiro de configuração que contém as definições de actualização do Kaspersky Anti-Virus. O ficheiro de configuração é um ficheiro em formato de texto que contém uma lista dos parâmetros da linha de comandos para a actualização da aplicação. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, são utilizados os valores de configuração definidos na interface da aplicação.
/APP=<on|off>	Activar / desactivar actualizações dos módulos da aplicação.

Exemplos:

- *Actualizar as bases de dados da aplicação e registar todos os eventos num relatório:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Actualizar os módulos do Kaspersky Anti-Virus, utilizando os parâmetros do ficheiro de configuração updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Uma amostra de um ficheiro de configuração:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt /app=on
```

REVERTER A ÚLTIMA ACTUALIZAÇÃO

Sintaxe do comando:

```
ROLLBACK [/R[A]:<ficheiro_relatório>] [/password=<sua_password>]
```

Descrição das definições:

/R[A]:<ficheiro_relatório>	**/R:**<ficheiro_relatório> – apenas regista eventos importantes no relatório. **/RA:**<ficheiro_relatório> – regista todos os eventos no relatório. Pode usar um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.
<sua_password>	A password da aplicação especificada na interface

Note que não pode executar este comando sem inserir a password.

Exemplo:

```
avp.com ROLLBACK /RA:rollback.txt /password=<sua_password>
```

EXPORTAR AS DEFINIÇÕES DE PROTECÇÃO

Sintaxe do comando:

```
avp.com EXPORT <perfil> <nomeficheiro>
```

Descrição das definições:

<perfil>	Componente ou tarefa com as definições a ser exportadas. Para a configuração **<perfil>**, pode utilizar qualquer valor especificado na secção de Ajuda "Gerir componentes e tarefas da aplicação".
<nomeficheiro>	Caminho para o ficheiro para o qual são exportadas as definições do Kaspersky Anti-Virus. Pode especificar um caminho absoluto ou relativo. O ficheiro de configuração é guardado em formato binário (*DAT*), se não tiver sido especificado outro formato ou se não estiver especificado de todo. Este pode ser usado mais tarde para importar definições da aplicação para outros computadores. O ficheiro de configuração também pode ser guardado como um ficheiro de texto. Para o fazer, digite a extensão *.txt* no nome do ficheiro. Note que não pode importar as definições de protecção a partir de um ficheiro de texto. Este ficheiro apenas pode ser usado para especificar as definições principais para o funcionamento do Kaspersky Anti-Virus.

Exemplo:

```
avp.com EXPORT c:\settings.dat
```

IMPORTAR AS DEFINIÇÕES DE PROTECÇÃO

Sintaxe do comando:

```
avp.com IMPORT <nomeficheiro>[/password=<sua_password>]
```

<nomeficheiro>	Caminho para o ficheiro a partir do qual serão importadas as definições do Kaspersky Anti-Virus. Pode especificar um caminho absoluto ou relativo.
<sua_password>	A password do Kaspersky Anti-Virus especificada na interface da aplicação. Só é possível importar os parâmetros de segurança a partir de um ficheiro binário.

Note que não pode executar este comando sem inserir a password.

Exemplo:

```
avp.com IMPORT c:\settings.dat /password=<sua_password>
```

INICIAR A APLICAÇÃO

Sintaxe do comando:

```
avp.com
```

PARAR A APLICAÇÃO

Sintaxe do comando:

```
EXIT /password=<sua_password>
```

<sua_password>	A password da aplicação especificada na interface

Note que não pode executar este comando sem inserir a password.

CRIAR UM FICHEIRO DE RASTREIO

Você pode precisar de criar um ficheiro de rastreio se tiver problemas com o Kaspersky Anti-Virus. Os ficheiros de rastreio são úteis para resolver problemas e são amplamente utilizados pelos especialistas do Suporte Técnico.

Sintaxe do comando:

```
avp.com TRACE [file] [on|off] [<nível_rastreio>]
```

Descrição das definições:

[on|off]	Activar/desactivar a criação do ficheiro de rastreio
[file]	Saída de rastreio para ficheiro
<nível_rastreio>	Este valor pode ser um número inteiro de 0 (nível mínimo, apenas mensagens críticas) a 700 (nível máximo, todas as mensagens). O Suporte Técnico dir-lhe-á que nível de rastreio necessita quando contactar o Suporte Técnico. Se isso não especificado, recomendamos que configure o nível para 500.

Apenas recomendamos a criação de ficheiros de rastreio para a resolução de um problema específico. A activação regular dos ficheiros de rastreio pode tornar o seu computador mais lento e encher o seu disco rígido.

Exemplos:

- *Para desactivar a criação de ficheiros de rastreio:*

```
avp.com TRACE file off
```

- *Para criar um ficheiro de rastreio para enviar ao Suporte Técnico com um nível de rastreio máximo de 500:*

```
avp.com TRACE file on 500
```

VISUALIZAR A AJUDA

Use este comando para visualizar a sintaxe da linha de comandos da aplicação:

```
avp.com [ /? | HELP ]
```

Para obter ajuda sobre a sintaxe de um comando específico, use um dos seguintes comandos:

```
avp.com <comando> /?
avp.com HELP <comando>
```

CÓDIGOS DE RETORNO DA INTERFACE DA LINHA DE COMANDOS

Esta secção contém uma lista dos códigos de retorno da linha de comandos. Os códigos gerais podem ser devolvidos por qualquer comando da linha de comandos. Os códigos de retorno incluem códigos gerais, assim como códigos específicos de um tipo de tarefa específico.

CÓDIGOS DE RETORNO GERAIS	
0	Operação concluída com sucesso
1	Valor de configuração inválido
2	Erro desconhecido
3	Erro de conclusão da tarefa
4	Tarefa cancelada
CÓDIGOS DE RETORNO DAS TAREFAS DE VERIFICAÇÃO DE VÍRUS	
101	Todos os objectos perigosos foram processados
102	Objectos perigosos detectados

ELIMINAR PROBLEMAS

Se ocorrerem problemas durante o funcionamento do Kaspersky Anti-Virus, primeiro deve verificar se o método para os resolver está descrito no sistema de Ajuda da aplicação ou na Base de Conhecimento da Kaspersky Lab em http://support.kaspersky.pt. A *Base de Conhecimento* é uma secção separada do site de Suporte Técnico e contém recomendações para os produtos da Kaspersky Lab, assim como respostas às perguntas mais frequentes. Tente utilizar este recurso para encontrar uma resposta à sua questão ou uma solução para o seu problema.

Para usar a Base de Conhecimento:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Suporte**.
3. Na janela **Suporte** que se abre, clique na ligação **Base de Conhecimento**.

Um outro recurso que pode utilizar para obter informação sobre como trabalhar com a aplicação é o Fórum de Utilizadores da Kaspersky Lab. É uma outra secção separada do site de Suporte Técnico e contém questões de utilizadores, informação de retorno e pedidos. Pode ver os principais tópicos do fórum, deixar comentários ou encontrar uma resposta a uma questão.

Para abrir o fórum de utilizadores:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Suporte**.
3. Na janela **Suporte** que se abre, clique na ligação **Fórum de Utilizadores**.

Se não conseguir encontrar uma solução para o seu problema no sistema de Ajuda, na Base de Conhecimento ou no Fórum de Utilizadores, recomendamos que contacte o Suporte Técnico da Kaspersky Lab.

NESTA SECÇÃO:

Criar um relatório sobre o estado do sistema 152

Criar um ficheiro de rastreio 153

Enviar ficheiros de dados 154

Executar script AVZ 155

CRIAR UM RELATÓRIO SOBRE O ESTADO DO SISTEMA

Para resolver os seus problemas, os especialistas da Kaspersky Lab poderão precisar de um relatório sobre o estado do sistema. Este relatório contém informação detalhada sobre os processos em execução, módulos e controladores carregados, extensões do Microsoft Internet Explorer e do Microsoft Windows Explorer, portas abertas, objectos suspeitos detectados, etc.

Quando é criado um relatório sobre o estado do sistema, não é recolhida qualquer informação pessoal do utilizador.

Para criar um relatório sobre o estado do sistema:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Suporte**.
3. Na janela **Suporte** que se abre, clique na ligação **Ferramentas de suporte**.
4. Na janela **Informação para Serviço de Suporte Técnico** que se abre, clique no botão **Criar relatório sobre estado do sistema**.

O relatório sobre o estado do sistema é criado nos formatos *HTML* e *XML* e será guardado no arquivo *sysinfo.zip*. Quando o processo de recolha de informação estiver concluído, pode ver o relatório.

Para ver o relatório:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Suporte**.
3. Na janela **Suporte** que se abre, clique na ligação **Ferramentas de suporte**.
4. Na janela **Informação para Serviço de Suporte Técnico** que se abre, clique no botão **Ver**.
5. Abra o arquivo *sysinfo.zip* que contém os ficheiros de relatório.

CRIAR UM FICHEIRO DE RASTREIO

Depois de instalar o Kaspersky Anti-Virus, podem ocorrer algumas falhas no sistema operativo ou no funcionamento de aplicações individuais. A causa mais provável é um conflito entre o Kaspersky Anti-Virus e o software instalado no seu computador ou com os controladores das componentes do seu computador. Pode-lhe ser pedido para criar um ficheiro de rastreio para os especialistas da Kaspersky Lab resolverem o seu problema com sucesso.

Para criar o ficheiro de rastreio:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Suporte**.
3. Na janela **Suporte** que se abre, clique na ligação **Ferramentas de suporte**.
4. Na janela **Informação para Serviço de Suporte Técnico** que se abre, use a lista suspensa na secção **Rastreios** para seleccionar o nível de rastreio. O nível de rastreio deve ser definido com base no aconselhamento do especialista do Suporte Técnico. Se não estiverem disponíveis indicações do Suporte Técnico, recomenda-se que defina o nível de rastreio para **500**.
5. Para iniciar o processo de rastreio, clique no botão **Activar**.
6. Reproduza a situação que causou o problema.
7. Para parar o processo de rastreio, clique no botão **Desactivar**.

Pode carregar os resultados de rastreio (ver secção "Enviar ficheiros de dados" na página 154) num servidor da Kaspersky Lab.

ENVIAR FICHEIROS DE DADOS

Depois de criar os ficheiros de rastreio e o relatório de estado do sistema, terá de enviá-los aos especialistas de suporte da Kaspersky Lab.

Irá precisar de um número de pedido para carregar os ficheiros de dados no servidor do Suporte Técnico. Este número está disponível no seu Arquivo Pessoal, no site de Suporte Técnico caso o seu pedido esteja activo.

Para carregar os ficheiros de dados no servidor do serviço de Suporte:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Suporte**.
3. Na janela **Suporte** que se abre, clique na ligação **Ferramentas de suporte**.
4. Na janela **Informação para Serviço de Suporte Técnico** que se abre, na secção **Acções**, clique no botão **Carregar informação no servidor para Serviço de Suporte Técnico**.
5. Na janela que se abre, assinale as caixas junto aos ficheiros de rastreio que deseja enviar para o Serviço de Suporte e clique no botão **Enviar**.
6. Na janela **Insira o número de pedido** que se abre, especifique o número atribuído ao seu pedido ao preencher o formulário electrónico no site do site do Serviço de Suporte.

Os ficheiros de rastreio seleccionados serão comprimidos e enviados para o servidor do Serviço de Suporte.

Se, por alguma razão, não conseguir contactar o Serviço de Suporte Técnico, pode guardar os ficheiros de dados no seu computador.

Para guardar os ficheiros de dados no disco:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Suporte**.
3. Na janela **Suporte** que se abre, clique na ligação **Ferramentas de suporte**.
4. Na janela **Informação para Serviço de Suporte Técnico** que se abre, na secção **Acções**, clique no botão **Carregar informação no servidor para Serviço de Suporte Técnico**.
5. Na janela que se abre, assinale as caixas junto aos ficheiros de rastreio que deseja enviar para o Serviço de Suporte e clique no botão **Enviar**.
6. Na janela **Insira o número de pedido** que se abre, clique no botão **Cancelar** e confirme que deseja guardar os ficheiros no disco.
7. Especifique o nome do arquivo na janela que se abre.

Mais tarde, poderá enviar os ficheiros guardados para o Suporte Técnico com a ajuda do Arquivo Pessoal (https://support.kaspersky.com/ru/personalcabinet?LANG=en).

EXECUTAR SCRIPT AVZ

Os especialistas da Kaspersky Lab irão analisar o seu problema através dos ficheiros de rastreio e do relatório sobre o estado do sistema. O resultado da análise é uma sequência de acções destinadas a eliminar os problemas detectados. Esta lista de acções pode ser muito longa.

Para simplificar o procedimento, são utilizados os scripts AVZ. Um script AVZ é um conjunto de instruções que permitem editar chaves de registo, colocar ficheiros na quarentena, procurar classes de ficheiros e ficheiros potencialmente colocados na quarentena relacionados com os mesmos, bloquear interceptores em Modo de Utilizador e em Modo de Núcleo, etc.

Para executar os scripts a aplicação inclui um *assistente de execução do script AVZ*. Este assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**; para fechar o assistente depois de este concluir o seu trabalho, utilize o botão **Concluir**. Para parar o assistente em qualquer altura, utilize o botão **Cancelar**.

Recomenda-se que não altere o texto de um script AVZ recebido dos especialistas da Kaspersky Lab. Se ocorrerem problemas durante a execução do script, por favor contacte o Serviço de Suporte Técnico.

Para iniciar o assistente:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Suporte**.
3. Na janela **Suporte** que se abre, clique na ligação **Ferramentas de suporte** na parte inferior da janela.
4. Na janela **Informação para Serviço de Suporte Técnico** que se abre, clique no botão **Executar AVZ script**.

Se o script for executado com sucesso, o assistente irá fechar-se. Se ocorrer um erro durante a execução do script, o assistente apresentará a respectiva mensagem de erro.

DECLARAÇÃO DE RECOLHA DE DADOS DO KASPERSKY SECURITY NETWORK

A. INTRODUÇÃO

Por favor, leia este documento com atenção. Este contém informação importante que deverá saber antes de continuar a utilizar os nossos serviços ou software. Caso continue a utilizar os serviços e software da Kaspersky Lab, considerar-se-á que aceita esta declaração de recolha de dados da Kaspersky Lab. Reservamos o direito de alterar esta Declaração de Recolha de Dados a qualquer altura, divulgando as alterações nesta página. Por favor, verifique a data de revisão abaixo indicada para determinar se a política foi alterada desde a última vez que a reviu. A utilização contínua de qualquer parte dos Serviços da Kaspersky Lab, após ter sido divulgada a Declaração de Recolha de Dados actualizada, será considerada como constituindo a sua aceitação das alterações.

A Kaspersky Lab e suas afiliadas (colectivamente, "Kaspersky Lab") criaram esta Declaração de Recolha de Dados para informar e divulgar as suas práticas de disseminação e recolha de dados para o Kaspersky Anti-Virus e Kaspersky Internet Security.

Algumas palavras da Kaspersky Lab

A Kaspersky Lab deposita grande empenho no fornecimento de serviços de qualidade superior a todos os nossos clientes e, em especial, no respeito pelas suas preocupações relativas à Recolha de Dados. Compreendemos que poderá ter dúvidas sobre a forma como o Kaspersky Security Network recolhe e utiliza informações e dados. Por isso, preparámos esta declaração para o informar sobre os princípios da Recolha de Dados que regulam o Kaspersky Security Network (a "Declaração de Recolha de Dados" ou "Declaração").

Esta Declaração de Recolha de Dados contém inúmeros detalhes gerais e técnicos sobre as medidas que tomamos para respeitar as suas preocupações relativas à Recolha de Dados. Organizámos esta Declaração de Recolha de Dados de acordo com os principais processos e áreas, de forma a que possa rapidamente rever as informações que mais lhe interessam. A questão central é que a satisfação das suas necessidades e expectativas constitui a base de tudo o que fazemos - incluindo a protecção na Recolha dos seus Dados.

Os dados e informações são recolhidos pela Kaspersky Lab. Depois de ter revisto esta Declaração de Recolha de Dados, se tiver dúvidas ou preocupações sobre a Recolha de Dados, por favor envie um e-mail para support@kaspersky.com.

O que é o Kaspersky Security Network?

O serviço Kaspersky Security Network permite que os utilizadores dos produtos de segurança da Kaspersky Lab, em todo o mundo, ajudem a facilitar a identificação e a reduzir o tempo que demora a fornecer protecção contra novos riscos de segurança ("que estão à solta") direccionados ao seu computador. Para identificar as novas ameaças e suas origens e para ajudar a melhorar a segurança do utilizador e a funcionalidade do produto, o Kaspersky Security Network recolhe determinados dados de segurança e da aplicação e envia esses dados à Kaspersky Lab para análise. Essas informações não contêm quaisquer informações pessoalmente identificáveis sobre o utilizador e são utilizadas pela Kaspersky Lab com o único propósito de melhorar os seus produtos de segurança e para fazer progredir as soluções contra ameaças e vírus maliciosos. No caso da transmissão acidental de quaisquer dados pessoais do utilizador, a Kaspersky Lab manterá e protegerá esses dados de acordo com esta Declaração de Recolha de Dados.

Ao participar no Kaspersky Security Network, você e os outros utilizadores dos produtos de segurança da Kaspersky Lab, em todo mundo, contribuem significativamente para ambiente mais seguro na Internet.

Questões Legais

O Kaspersky Security Network pode estar sujeito às leis de diversas jurisdições, uma vez que os seus serviços podem ser utilizados em diferentes jurisdições, incluindo os Estados Unidos da América. A Kaspersky Lab revelará informações pessoalmente identificáveis sem a sua autorização, quando exigido por lei ou quando acreditar, de boa-fé, que tal acção seja necessária para investigar ou proteger contra actividades danosas os hóspedes, visitantes, associados ou propriedades da Kaspersky Lab ou de outros. Tal como acima mencionado, as leis relacionadas com os dados e informações recolhidos pelo Kaspersky Security Network podem variar entre países. Por exemplo, algumas informações pessoalmente identificáveis recolhidas na União Europeia e nos seus Estados-Membros estão sujeitas às Directivas da UE relativas a dados pessoais, Privacidade e comunicações electrónicas incluindo, mas não exclusivamente, a Directiva

2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da Privacidade no sector das comunicações electrónicas e a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e as leis posteriormente adoptadas nos Estados-Membros da UE, a Decisão 2001/497/CE da Comissão Europeia relativa às cláusulas contratuais-tipo (transferência de dados pessoais para países terceiros) e as leis posteriormente adoptadas nos Estados-Membros da UE.

O Kaspersky Security Network deverá informar devidamente os utilizadores em questão, quando começar a recolher as informações acima mencionadas, sobre qualquer partilha dessas informações, nomeadamente para uso no desenvolvimento de negócios, e deverá permitir que estes utilizadores da Internet comuniquem via on-line a opção de inclusão (nos Estados-Membros da UE e outros países que requeiram o procedimento de inclusão) ou de exclusão (para todos os outros países) da utilização comercial destes dados e/ou da transmissão destes dados a terceiros.

A Kaspersky Lab pode ser obrigada, pelas autoridades de aplicação da lei ou judiciais, a fornecer informações pessoalmente identificáveis às autoridades governamentais adequadas. Se exigido pelas autoridades de aplicação da lei ou judiciais, forneceremos estas informações após recepção da documentação adequada. A Kaspersky Lab também pode fornecer informações às autoridades de aplicação da lei para proteger as suas propriedades e a saúde e segurança dos indivíduos, tal como permitido pelos estatutos.

As declarações às autoridades dos Estados-Membros em matéria de Protecção de Dados Pessoais serão feitas de acordo com as leis posteriormente em vigor nos Estados-Membros da UE. A informação sobre essas declarações estará acessível nos serviços do Kaspersky Security Network.

B. INFORMAÇÕES RECOLHIDAS

Dados Que Recolhemos

Os utilizadores têm direito a conceder dados de acordo com esta declaração e o serviço Kaspersky Security Network irá recolher e enviar dados centrais e alargados à Kaspersky Lab sobre potenciais riscos de segurança direccionados ao seu computador. Os dados recolhidos incluem:

- Dados Centrais:
    - informação sobre o hardware e software do seu computador, incluindo o sistema operativo e service packs instalados, objectos do núcleo, controladores, serviços, extensões do Internet Explorer, extensões de impressão, extensões do Windows Explorer, ficheiros de programa transferidos, elementos de configuração activa, aplicativos do painel de controlo, registos do ficheiro anfitriões e do registo, endereços IP, tipos de navegador, clientes de e-mail e o número da versão do produto da Kaspersky Lab, que normalmente não é pessoalmente identificável;
    - uma ID única que é gerada pelo produto da Kaspersky Lab para identificar máquinas individuais sem identificar o utilizador e que não contém quaisquer informações pessoais;
    - informação sobre o estado da protecção antivírus do seu computador e dados sobre quaisquer ficheiros ou actividades suspeitos de serem maliciosos (por exemplo, nome do vírus, data/hora da detecção, nomes/caminhos e tamanho dos ficheiros infectados, endereço IP e porta do ataque de rede, nome da aplicação suspeita de ser maliciosa). Por favor, tenha em atenção que os dados recolhidos acima indicados não contêm informações pessoalmente identificáveis.
- Dados Alargados:
    - informação sobre aplicações digitalmente assinadas transferidas pelo utilizador (URL, tamanho do ficheiro, nome do signatário);
    - informação sobre aplicações executáveis (tamanho, atributos, data de criação, informação sobre cabeçalhos PE, região, nome, localização e utilitário de compressão utilizado).
- Ficheiros e/ou suas partes. O serviço Kaspersky Security Network pode recolher e enviar ficheiros inteiros e/ou suas partes à Kaspersky Lab para análise adicional. A transferências de ficheiros e/ou suas partes apenas são executadas se a Declaração de Recolha de Dados da Kaspersky Lab tiver sido aceite por si.

Proteger a Transmissão e Armazenamento de Dados

A Kaspersky Lab está empenhada em proteger a segurança das informações que recolhe. As informações recolhidas são armazenadas em servidores de computador com acesso limitado e controlado. A Kaspersky Lab opera redes de dados seguras protegidas por firewalls normalizadas e sistemas de protecção por password. A Kaspersky Lab utiliza uma ampla gama de tecnologias e procedimentos de segurança para proteger as informações recolhidas contra ameaças como o acesso, utilização ou divulgação não-autorizados. As nossas políticas de segurança são regularmente revistas e, se necessário, melhoradas e apenas os indivíduos autorizados têm acesso aos dados que recolhemos. A Kaspersky Lab toma medidas para garantir que as suas informações são tratadas de forma segura e de acordo com esta Declaração. Infelizmente, não é possível garantir a segurança total de qualquer transmissão de dados. Como resultado, embora nos esforcemos por proteger os seus dados, não podemos garantir a segurança de quaisquer dados que nos transmita ou a partir dos nossos produtos ou serviços, incluindo sem limitação o Kaspersky Security Network, e você utiliza todos esses serviços por sua conta e risco.

Os dados que são recolhidos podem ser transferidos para os servidores da Kaspersky Lab e a Kaspersky Lab tomou as precauções necessárias para garantir que as informações recolhidas, se transferidas, recebem o nível adequado de protecção. Tratamos os dados que recolhemos como informações confidenciais. Estes são adequadamente sujeitos aos nossos procedimentos de segurança e políticas empresariais relativas à protecção e utilização de informações confidenciais. Depois dos dados recolhidos chegarem à Kaspersky Lab, estes são armazenados num servidor com funcionalidades de segurança física e electrónica normalizadas, incluindo a utilização de procedimentos de início de sessão/password e firewalls electrónicas concebidas para bloquear o acesso não-autorizado a partir do exterior da Kaspersky Lab. Os dados recolhidos pelo Kaspersky Security Network abrangidos por esta Declaração são processados e armazenados nos Estados Unidos e possivelmente noutras jurisdições e também noutros países onde a Kaspersky Lab exerce actividade. Todos os funcionários da Kaspersky Lab estão conscientes das nossas políticas de segurança. Os seus dados só estão acessíveis aos funcionários que deles necessitam para desempenharem as suas funções. Todos os dados armazenados não serão associados a quaisquer informações pessoalmente identificáveis. A Kaspersky Lab não combina os dados armazenados pelo Kaspersky Security Network com quaisquer dados, listas de contacto ou informações de subscrição recolhidas pela Kaspersky Lab para fins promocionais ou outros.

C. UTILIZAÇÃO DOS DADOS RECOLHIDOS

Como São Utilizadas As Suas Informações Pessoais

A Kaspersky Lab recolhe os dados por forma a analisar e identificar as fontes de potenciais riscos de segurança e para melhorar a capacidade dos produtos da Kaspersky Lab na detecção de comportamentos maliciosos, sites fraudulentos, softwares criminosos e outros tipos de ameaças de segurança na Internet para fornecer o melhor nível de protecção possível aos clientes da Kaspersky Lab no futuro.

Divulgação de Informações a Terceiros

A Kaspersky Lab pode revelar quaisquer informações recolhidas se tal for solicitado por um oficial responsável pela aplicação da lei, tal como exigido ou permitido por lei, ou em resposta a uma intimação ou outro processo legal ou se acreditarmos de boa-fé que o devemos fazer para cumprir com a lei, regulamento, uma intimação ou outro processo legal aplicável ou um pedido executório governamental. A Kaspersky Lab também pode revelar informações pessoalmente identificáveis quando tiver razões para acreditar que a divulgação dessa informação é necessária para identificar, contactar ou actuar legalmente contra alguém que possa estar a violar esta Declaração, os termos dos seus acordos com a Empresa ou para proteger a segurança dos nossos utilizadores e do público ou ao abrigo de acordos de confidencialidade e licenciamento com determinados terceiros que nos dão assistência no desenvolvimento, operação e manutenção do Kaspersky Security Network. Para promover o conhecimento, detecção e prevenção dos riscos de segurança na Internet, a Kaspersky Lab pode partilhar determinadas informações com organizações de investigação e outros fornecedores de software de segurança. A Kaspersky Lab também pode utilizar as estatísticas derivadas das informações recolhidas para controlar e publicar relatórios sobre a evolução dos riscos de segurança.

As escolhas à sua disposição

A participação no Kaspersky Security Network é opcional. Você pode activar e desactivar o serviço Kaspersky Security Network em qualquer altura, acedendo às configurações da Informação de Retorno na página de opções do seu produto da Kaspersky Lab. Contudo, por favor tenha em atenção que se escolher desactivar o serviço Kaspersky Security Network, poderemos não ser capazes de lhe fornecer alguns dos serviços dependentes da recolha desses dados. Depois de terminar o período de serviço do seu produto da Kaspersky Lab, algumas das funções do software da Kaspersky Lab podem continuar a funcionar, mas as informações deixarão de ser, automaticamente, enviadas para a Kaspersky Lab.

Também reservamos o direito de enviar mensagens de alerta esporádicas aos utilizadores para os informar sobre alterações específicas que possam afectar a sua capacidade para utilizar os nossos serviços que subscreveram

previamente. Também reservamos o direito de o contactar se a tal formos obrigados como parte de um procedimento legal ou se tiver ocorrido uma violação de quaisquer acordos aplicáveis de licenciamento, garantia e compra.

A Kaspersky Lab conserva estes direitos porque, em casos limitados, sentimos que poderemos necessitar do direito de contactá-lo por questões legais ou em relação a assuntos que podem ser importantes para si. Estes direitos não nos permitem contactá-lo para comercializar serviços novos ou já existentes, caso nos tenha solicitado para não o fazermos, e a emissão destes tipos de comunicação é rara.

D. RECOLHA DE DADOS – PEDIDOS E RECLAMAÇÕES RELACIONADAS

A Kaspersky Lab recebe e trata, com o máximo respeito e atenção, as preocupações dos seus utilizadores sobre a Recolha de Dados. Se detectar alguma situação de incumprimento desta Declaração, no que respeita aos seus dados e informações, ou se tiver outros pedidos ou preocupações relacionadas, pode escrever ou contactar a Kaspersky Lab através do e-mail: support@kaspersky.com.

Na sua mensagem, por favor descreva, o mais detalhadamente possível, a natureza do seu pedido. Investigaremos o seu pedido ou reclamação com a maior rapidez possível.

O fornecimento de informações é voluntário. Uma opção de recolha de dados pode ser desactivada pelo utilizador, a qualquer altura, na secção "Informação de Retorno" na página "Configuração" de qualquer produto Kaspersky adequado.

© 1997-2009 Kaspersky Lab ZAO. Todos os direitos reservados.

UTILIZAR CÓDIGO DE TERCEIROS

Foi utilizado código de terceiros durante a criação do Kaspersky Anti-Virus.

NESTA SECÇÃO:

Biblioteca Crypto C (biblioteca de software de segurança de dados) 161

Biblioteca Fastscript 1.9 161

Biblioteca Libnkfm 7.4.7.7 161

Biblioteca GNU bison parser 162

Biblioteca AGG 2.4 162

Biblioteca OpenSSL 0.9.8d 163

Biblioteca Gecko SDK 1.8 164

Biblioteca Zlib 1.2 164

Biblioteca Libpng 1.2.8, 1.2.29 164

Biblioteca Libnkfm 2.0.5 164

Biblioteca Expat 1.2, 2.0.1 165

Biblioteca Info-ZIP 5.51 165

Biblioteca Windows Installer XML (WiX) 2.0 166

Biblioteca Passthru 168

Biblioteca Filter 168

Biblioteca Netcfg 169

Biblioteca Pcre 3.0 169

Biblioteca RFC1321-based (RSA-free) MD5 169

Biblioteca Windows Template Library (WTL 7.5) 169

Biblioteca Libjpeg 6b 172

Biblioteca Libungif 3.0 173

Biblioteca Libxdr 173

Biblioteca Tiniconv - 1.0.0 174

Biblioteca Bzip2/libbzip2 1.0.5 179

Biblioteca Libspf2-1.2.9 179

Biblioteca Protocol Buffer 180

BIBLIOTECA CRYPTO C (BIBLIOTECA DE SOFTWARE DE SEGURANÇA DE DADOS)

Para criar e verificar as assinaturas digitais, é utilizada a biblioteca de software de segurança de dados Crypto C, desenvolvida pela "CryptoEX", http://www.cryptoex.ru.

BIBLIOTECA FASTSCRIPT 1.9

Durante a criação da aplicação foi utilizada a Biblioteca FastScript. Copyright © Fast Reports Inc. Todos os direitos reservados.

BIBLIOTECA LIBNKFM 7.4.7.7

Para criar a aplicação foi utilizada a Biblioteca pcre 7.4 copyright © 1997-2008 University of Cambridge, de acordo com a licença BSD.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" license, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTECA GNU BISON PARSER

Durante a criação da aplicação foi utilizada a Biblioteca bison parser skeleton 2.3 copyright © GNU Project http://ftp.gnu.org/gnu/bison/, ao abrigo da estrutura de uma excepção especial.

As a special exception, you may create a larger work that contains part or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BIBLIOTECA AGG 2.4

Durante a criação da aplicação foi utilizada a Biblioteca AGG (Anti-Grain Geometry) 2.4 copyright © 2002-2005 Maxim Shemanarev. All rights reserved, de acordo com a licença BSD alterada.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BIBLIOTECA OPENSSL 0.9.8D

Durante a criação da aplicação foi utilizada a Biblioteca OpenSSL 0.9.8d copyright © 1998-2007 The OpenSSL Project. All rights reserved, de acordo com as licenças OpenSSL License e Original SSLeay License (http://www.openssl.org/).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

BIBLIOTECA GECKO SDK 1.8

Durante a criação da aplicação foi utilizada a Biblioteca Gecko SDK 1.8 Copyright © Mozilla Foundation. All rights reserved, de acordo com a licença MPL 1.1 (http://www.mozilla.org/MPL/MPL-1.1.html). Site da Internet e ligação para o pacote de distribuição: http://developer.mozilla.org/en/docs/Gecko_SDK.

BIBLIOTECA ZLIB 1.2

Durante a criação da aplicação foi utilizada a Biblioteca zlib 1.2 copyright © 1995-2005 Jean-loup Gailly and Mark Adler. All rights reserved, de acordo com a licença zlib/libpng.

BIBLIOTECA LIBPNG 1.2.8, 1.2.29

Durante a criação da aplicação foi utilizada a Biblioteca libpng 1.2.8, 1.2.29 copyright © 2004, 2006-2008 Glenn Randers-Pehrson. All rights reserved, de acordo com a licença zlib/libpng.

BIBLIOTECA LIBNKFM 2.0.5

Durante a criação da aplicação foi utilizada a Biblioteca libnkfm 2.0.5 Copyright (c) KUBO Takehiro. Todos os direitos reservados.

BIBLIOTECA EXPAT 1.2, 2.0.1

Durante a criação da aplicação foi utilizada a Biblioteca Expat 1.2, 2.0.1 Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. All rights reserved, utilizada de acordo com as seguintes condições:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTECA INFO-ZIP 5.51

Durante a criação da aplicação foi utilizada a Biblioteca Info-ZIP 5.51 Copyright (c) 1990-2007. All rights reserved, de acordo com a licença Info-ZIP.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip", "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "UnZipSFX", "WiZ", "Pocket UnZip", "Pocket Zip", and "MacZip" for its own source and binary releases.

BIBLIOTECA WINDOWS INSTALLER XML (WIX) 2.0

Durante a criação da aplicação foi utilizada a Biblioteca Windows Installer XML (WiX) 2.0 Copyright (c) Microsoft Corporation. All rights reserved, de acordo com a licença CPL 1.0 (http://sourceforge.net/projects/wix/).

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

   i) changes to the Program, and

   ii) additions to the Program;

   where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

   a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

   b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

   c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

   d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTECA PASSTHRU

Durante a criação da aplicação foi utilizada a Biblioteca Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation. All rights reserved.

BIBLIOTECA FILTER

Durante a criação da aplicação foi utilizada a Biblioteca Ndis Sample NDIS Lightweight filter driver Copyright (c) 2004-2005 Microsoft Corporation. All rights reserved.

BIBLIOTECA NETCFG

Durante a criação da aplicação foi utilizada a Biblioteca Network Configuration Sample Copyright (c) 1997 Microsoft Corporation. All rights reserved.

BIBLIOTECA PCRE 3.0

Durante a criação da aplicação foi utilizada a Biblioteca pcre 3.0 copyright © 1997-1999 University of Cambridge, de acordo com a licença PCRE LICENSE. All rights reserved.

BIBLIOTECA RFC1321-BASED (RSA-FREE) MD5

Durante a criação da aplicação foi utilizada a Biblioteca RFC1321-based (RSA-free) MD5. Copyright (c) 1999, 2002 Aladdin Enterprises. All rights reserved. Distribuída ao abrigo da licença zlib/libpng.

BIBLIOTECA WINDOWS TEMPLATE LIBRARY (WTL 7.5)

Durante a criação da aplicação foi utilizada a Biblioteca Windows Template Library 7.5 Copyright (c) 2005 Microsoft Corporation. All rights reserved, de acordo com a licença Common Public license 1.0, http://sourceforge.net/projects/wtl/.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

   i) changes to the Program, and

   ii) additions to the Program;

   where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTECA LIBJPEG 6B

Durante a criação da aplicação foi utilizada a Biblioteca libjpeg 6b. Copyright (c) 1991-1998, Thomas G. Lane. All Rights. É utilizada de acordo com as seguintes condições:

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

BIBLIOTECA LIBUNGIF 3.0

Durante a criação da aplicação foi utilizada a Biblioteca libungif 3.0. Copyright (c) 1997 Eric S. Raymond. É utilizada de acordo com as seguintes condições:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTECA LIBXDR

Durante a criação da aplicação foi utilizada a Biblioteca libxdr copyright © Sun Microsystems, Inc.. É utilizada de acordo com as seguintes condições:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

BIBLIOTECA TINICONV - 1.0.0

Durante a criação da aplicação foi utilizada a Biblioteca tiniconv – 1.0.0. Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (http://sourceforge.net/projects/tiniconv/), de acordo com a licença GNU LGPL 2.1 (http://www.gnu.org/).

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary

General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

BIBLIOTECA BZIP2/LIBBZIP2 1.0.5

Durante a criação da aplicação foi utilizada a Biblioteca bzip2/libbzip2 1.0.5. Copyright (C) 1996-2007 Julian R Seward. All rights reserved. É utilizada de acordo com as seguintes condições:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

BIBLIOTECA LIBSPF2-1.2.9

Durante a criação da aplicação foi utilizada a Biblioteca libspf2-2/1/09. Copyright 2005 by Shevek and Wayne Schlitt. All rights reserved, utilizada de acordo com as condições da licença The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTECA PROTOCOL BUFFER

Durante a criação da aplicação foi utilizada a Biblioteca Protocol Buffer. Copyright 2008, Google Inc. All rights reserved, é distribuída de acordo com as condições da licença New BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

GLOSSÁRIO

Esta definición no tiene titular Lista de máscaras e endereços de recursos da Internet, em cujos conteúdos o utilizador confia. A aplicação da Kaspersky Lab não verifica páginas de Internet, correspondentes a algum item da lista, quanto à presença de objectos maliciosos.

ACTIVAR A APLICAÇÃO

O procedimento de activação da aplicação consiste em inserir um código de activação e obter uma chave que permitirá à aplicação determinar se o utilizador tem direitos suficientes para a utilizar e descobrir a data de validade da licença.

ACTUALIZAÇÃO

O procedimento de substituição/adição de novos ficheiros (bases de dados ou módulos da aplicação) recolhidos a partir dos servidores de actualização da Kaspersky Lab.

ACTUALIZAÇÕES DA BASE DE DADOS

Uma das funções executadas por uma aplicação da Kaspersky Lab que lhe permite manter a protecção actual. Ao fazê-lo, as bases de dados são transferidas dos servidores de actualização da Kaspersky Lab para o computador e estão automaticamente ligadas à aplicação.

ACTUALIZAÇÕES DISPONÍVEIS

Um conjunto de actualizações dos módulos da aplicação da Kaspersky Lab, incluindo actualizações críticas acumuladas ao longo de um período de tempo e alterações na arquitectura da aplicação.

ACTUALIZAÇÕES URGENTES

Actualizações críticas dos módulos da aplicação da Kaspersky Lab.

ANALISADOR HEURÍSTICO

Tecnologias de detecção de ameaças para ameaças que não podem ser detectadas através das bases de dados Antivírus. Permite detectar objectos suspeitos de estarem infectados com um vírus desconhecido ou com uma variante de um vírus conhecido.

A utilização do analisador heurístico detecta até 92% das ameaças. Este mecanismo é razoavelmente eficaz e muito raramente conduz a falsos alarmes.

Os ficheiros detectados pelo analisador heurístico são considerados suspeitos.

APAGAR UM OBJECTO

O método de processamento de objectos que os apaga fisicamente da sua localização original (disco rígido, pasta, recurso de rede). Recomendamos que aplique este método aos objectos perigosos que, por qualquer razão, não possam ser desinfectados.

APLICAÇÃO INCOMPATÍVEL

Uma aplicação antivírus de um fabricante terceiro ou uma aplicação da Kaspersky Lab que não suporta a gestão através do Kaspersky Administration Kit.

ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA

Área de armazenamento especial concebida para guardar cópias de segurança de objectos criadas antes da sua primeira desinfecção ou eliminação.

ARQUIVO

Ficheiro que "contém" um ou vários outros objectos que também podem ser arquivos.

BASE DE ENDEREÇOS DE INTERNET SUSPEITOS

Lista de endereços de Internet, cujo conteúdo pode ser considerado potencialmente perigoso. A lista é criada pelos especialistas da Kaspersky Lab. É regularmente actualizada e está incluída no pacote da aplicação da Kaspersky Lab.

BASE DE ENDEREÇOS DE PHISHING

Lista de endereços de Internet, que são definidos como endereços de phishing por parte dos especialistas da Kaspersky Lab. A base é regularmente actualizada e faz parte da aplicação da Kaspersky Lab.

BASES DE DADOS

Bases de dados criadas pelos especialistas da Kaspersky Lab e que contêm uma descrição detalhada de todas as ameaças da segurança do computador actualmente conhecidas, assim como os métodos usados para a sua detecção e desinfecção. Estas bases de dados são constantemente actualizadas pela Kaspersky Lab, à medida que aparecem novas ameaças. Para atingir uma melhor qualidade na detecção de ameaças, recomendamos que copie regularmente as bases de dados dos servidores de actualização da Kaspersky Lab.

BASES DE DADOS DE E-MAIL

Bases de dados que contêm e-mails num formato especial e guardadas no seu computador. Cada e-mail de entrada/saída é colocado na base de dados de e-mails depois de ser recebido/enviado. Estas bases de dados são verificadas durante uma verificação completa do computador.

No momento em que são recebidos e enviados, os e-mails de entrada e de saída são analisados, em tempo real, quanto à presença de vírus, caso a protecção em tempo real esteja activada.

BLOQUEAR O OBJECTO

Recusar o acesso a um objecto por parte de aplicações externas. Um objecto bloqueado não pode ser lido, executado, alterado ou apagado.

CABEÇALHO

A informação no início de um ficheiro ou mensagem, que contém dados de baixo nível sobre o estado e processamento do ficheiro (ou mensagem). Em particular, o cabeçalho de uma mensagem de e-mail contém dados como a informação sobre o remetente e o destinatário, assim como a data.

CERTIFICADO DO SERVIDOR DE ADMINISTRAÇÃO

Certificado que permite a autenticação do Servidor de Administração, ao ligar a Consola de Administração ao mesmo e ao trocar dados com computadores de utilizadores. O certificado do servidor de administração é criado com a instalação do Servidor de Administração e é guardado na subpasta Cert da pasta de instalação da aplicação.

CONFIGURAÇÕES DA APLICAÇÃO

Configurações da aplicação que são comuns a todos os tipos de tarefas, regulando o funcionamento da aplicação como um todo, tais como as configurações de desempenho da aplicação, as configurações de relatórios, configurações do armazenamento de cópias de segurança.

CONFIGURAÇÕES DE TAREFAS

Configurações da aplicação que são específicas para cada tipo de tarefa.

CONTADOR DE SURTOS DE VÍRUS

Modelo, com base no qual é gerada uma notificação sobre uma ameaça de surto de vírus. O contador de surtos de vírus inclui uma combinação de definições que determinam o limite de actividade de vírus, a forma de propagação e o texto das mensagens a enviar.

CÓPIA DE SEGURANÇA

Criar uma cópia de segurança de um ficheiro antes de qualquer processamento e colocar a cópia na área de armazenamento de cópias de segurança, com a possibilidade de restaurar o ficheiro mais tarde, por exemplo para o verificar com as bases de dados actualizadas.

DESINFECÇÃO DE OBJECTOS

O método utilizado para o processamento de objectos infectados que resulta na recuperação completa ou parcial de dados ou na decisão de que os objectos não podem ser desinfectados. A desinfecção de objectos é efectuada, utilizando os registos da base de dados. Parte dos dados podem ser perdidos durante a desinfecção.

DESINFECTAR OBJECTOS APÓS REINICIALIZAÇÃO

Um método de processamento dos objectos infectados que estão a ser utilizados por outras aplicações no momento da desinfecção. Este método cria uma cópia do objecto infectado, desinfecta a cópia criada e, após a próxima reinicialização do sistema, substitui o objecto original infectado pela cópia desinfectada.

ESTADO DE PROTECÇÃO

O estado actual de protecção, que resume o nível de segurança do computador.

EXCLUSÃO

Uma exclusão é um objecto excluído da verificação pela aplicação da Kaspersky Lab. Você pode excluir da verificação os ficheiros de determinados formatos, utilizando uma máscara de ficheiro, ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objectos segundo o tipo de ameaça, de acordo com a classificação da Enciclopédia de Vírus. A cada tarefa pode ser atribuído um conjunto de exclusões.

FICHEIRO COMPRIMIDO

Um arquivo que contém um programa de descompressão e instruções para o sistema operativo para o executar.

FICHEIRO DA CHAVE

Ficheiro com a extensão .key, que constitui a sua "chave " pessoal, necessário para trabalhar com a aplicação da Kaspersky Lab. Um ficheiro da chave está incluído no produto, caso o tenha adquirido junto dos distribuidores da Kaspersky Lab, ou é-lhe enviado por e-mail, caso tenha adquirido o produto on-line.

FLUXOS NTFS ALTERNADOS

Fluxos de dados NTFS (fluxos de dados alternados) concebidos para conterem atributos adicionais ou informação de ficheiros.

Cada ficheiro no sistema de ficheiros NTFS é um conjunto de fluxos. Um desses fluxos contém os conteúdos do ficheiro que é possível visualizar depois de abrir o ficheiro, outros fluxos (chamados alternados) foram concebidos para conter meta-informação e garantir, por exemplo, a compatibilidade do NTFS com outros sistemas, tais como um sistema de ficheiros Macintosh mais antigo, denominado de Hierarchical File System (HFS) ou sistema de ficheiros hierárquico. Os fluxos podem ser criados, apagados, armazenados em separado, renomeados e inclusive executados como um processo.

Os fluxos alternados podem ser utilizados por intrusos para transferirem dados de forma secreta ou para roubá-los de um computador.

GATEWAY

Computador equipado com dois adaptadores de rede (cada um dos quais ligados a diferentes redes) que transferem dados de uma rede para outra.

INSTALAÇÃO COM UM CENÁRIO DE INICIALIZAÇÃO

Método de instalação remota das aplicações da Kaspersky Lab, que permite atribuir a inicialização da tarefa de instalação remota a uma conta de utilizador individual (ou a diversas contas de utilizador). O registo de um utilizador num domínio resulta numa tentativa para instalar a aplicação num computador cliente, no qual o utilizador foi registado. Este método é recomendado para instalar as aplicações em computadores com os sistemas operativos Microsoft Windows 98 / Me.

INTERCEPTOR

Subcomponente da aplicação, responsável por verificar tipos específicos de e-mails. O conjunto de interceptores específicos da sua instalação depende do papel ou combinação de papéis para os quais a aplicação está a ser implementada.

LICENÇA ACTIVA

A licença actualmente utilizada para o funcionamento da aplicação da Kaspersky Lab. A licença define a data de validade para a funcionalidade completa e a política de licenciamento para a aplicação. A aplicação não pode ter mais do que uma licença com o estado activa.

LICENÇA ADICIONAL

Uma licença que foi adicionada para o funcionamento da aplicação da Kaspersky Lab, mas que não foi activada. A licença adicional entra em vigor quando a licença activa expirar.

LIMITE DE ACTIVIDADE DE VÍRUS

O nível máximo permissível de um tipo específico de eventos ao longo de um período de tempo limitado que, quando excedido, será considerado como actividade excessiva de vírus e como ameaça de um surto de vírus. Esta característica é importante durante os surtos de vírus e permite ao administrador reagir, de forma atempada, às ameaças de surtos de vírus que possam surgir.

LISTA DE ENDEREÇOS VERIFICADOS

Lista de máscaras e endereços de recursos da Internet, que são obrigatoriamente verificados pela aplicação da Kaspersky Lab, quanto à presença de objectos maliciosos.

LISTA NEGRA DE FICHEIROS DE CHAVE

Uma base de dados que contém informação sobre ficheiros de chave da Kaspersky Lab que estão na lista negra e cujos proprietários violaram os termos do contrato de licença e informação sobre ficheiros de chave que foram emitidos mas que, por alguma razão, não foram vendidos ou foram substituídos. Um ficheiro da lista negra é necessário para o funcionamento das aplicações da Kaspersky Lab. Os conteúdos do ficheiro são actualizados juntamente com as bases de dados.

MÁSCARA DE FICHEIRO

Representação do nome e extensão de um ficheiro, utilizando meta caracteres. Os dois meta caracteres normalmente utilizados nas máscaras de ficheiro são * e ?, onde * representa qualquer número de caracteres e ? representa qualquer caractere único. Ao utilizar estes meta caracteres, você pode representar qualquer ficheiro. Note que o nome e a extensão estão sempre separados por um ponto ".".

MODELO DE NOTIFICAÇÃO

Modelo com base no qual é gerada uma notificação sobre objectos infectados detectados pela verificação. O modelo de notificação inclui uma combinação de definições que regulam o modo de notificação, a forma de propagação e o texto das mensagens a enviar.

MÓDULOS DA APLICAÇÃO

Ficheiros incluídos no pacote de instalação da Kaspersky Lab, responsáveis por executar as principais tarefas da aplicação. Um módulo executável específico corresponde a cada tipo de tarefa executada pela aplicação (protecção em tempo real, verificação sob pedido, actualizações). Ao executar uma verificação completa do seu computador a partir da janela principal, você inicia a execução do módulo desta tarefa.

MOVER OBJECTOS PARA A QUARENTENA

O método de processamento de um objecto potencialmente infectado, bloqueando o acesso ao ficheiro e movendo-o da sua localização original para a pasta da Quarentena, onde o objecto é guardado na forma encriptada, o que exclui a ameaça de infecção.

NÍVEL DE GRAVIDADE DOS EVENTOS

Descrição do evento, registado durante o funcionamento da aplicação da Kaspersky Lab. Existem quatro níveis de gravidade:

Evento crítico.

Falha funcional.

Aviso.

Mensagem informativa.

Os eventos do mesmo tipo podem ter diferentes níveis de gravidade, dependendo da situação em que o evento ocorreu.

NÍVEL DE SEGURANÇA

O nível de segurança é definido como uma configuração predefinida para uma componente.

NÍVEL RECOMENDADO

Nível de Segurança baseado nas configurações da aplicação recomendadas pelos especialistas da Kaspersky Lab para fornecer o nível óptimo de protecção para o seu computador. Este nível está definido para ser utilizado por defeito.

OBJECTO INFECTADO

Objecto que contém código malicioso. É detectado quando uma secção do código do objecto corresponde na totalidade a uma secção do código de uma ameaça conhecida. A Kaspersky Lab recomenda que não utilize esses objectos uma vez que podem levar à infecção do seu computador.

OBJECTO OLE

Um objecto anexado ou um objecto incorporado noutro ficheiro. A aplicação da Kaspersky Lab permite verificar os objectos OLE quanto à presença de vírus. Por exemplo, se inserir uma tabela do Microsoft Excel num documento do Microsoft Office Word, a tabela será verificada como um objecto OLE.

OBJECTO PERIGOSO

Objecto que contém um vírus. Recomenda-se que não aceda a estes objectos, uma vez que isso pode resultar na infecção do seu computador. Quando for detectado um objecto infectado, recomendamos que o desinfecte utilizando uma das aplicações antivírus da Kaspersky Lab ou que o apague se a desinfecção não for possível.

OBJECTO POTENCIALMENTE INFECTADO

Um objecto que contém código alterado de um vírus conhecido ou código que se assemelha ao código de um vírus, mas ainda desconhecido pela Kaspersky Lab. Os ficheiros potencialmente infectados são detectados através do analisador heurístico.

OBJECTO POTENCIALMENTE INFECTÁVEL

Um objecto que, devido à sua estrutura ou formato, pode ser utilizado por intrusos como um "recipiente" para armazenar e distribuir um objecto malicioso. Por norma, estes objectos são ficheiros executáveis, por exemplo ficheiros com as extensões .com, .exe, .dll, etc. O risco de activação do código malicioso nesses ficheiros é relativamente elevado.

OBJECTO SUSPEITO

Um objecto que contém código alterado de um vírus conhecido ou código que se assemelha ao código de um vírus, mas ainda desconhecido pela Kaspersky Lab. Os objectos suspeitos são detectados através do analisador heurístico.

OBJECTOS DE INICIALIZAÇÃO

O conjunto de programas necessários para iniciar e utilizar correctamente o sistema operativo e o software instalado no seu computador. Estes objectos são executados sempre que o sistema operativo é iniciado. Existem vírus capazes de infectar especificamente esses objectos, podendo levar, por exemplo, ao bloqueio do seu acesso ao sistema operativo.

PACOTE DE ACTUALIZAÇÃO

Pacote de ficheiros para actualizar o software. É transferido a partir da Internet e instalado no seu computador.

PERÍODO DE VALIDADE DA LICENÇA

Período de tempo, durante o qual você pode utilizar todas as funcionalidades da sua aplicação da Kaspersky Lab. O período de validade da licença normalmente corresponde a um ano, a contar da data da sua instalação. Depois de a licença expirar, a aplicação terá funcionalidades reduzidas. Você não poderá actualizar as bases de dados da aplicação.

PORTA DE ENTRADA/SAÍDA

Serve nos processadores (tais como Intel) para o intercâmbio de dados com as componentes de hardware. A porta de entrada/saída está associada a uma determinada componente de hardware e permite que as aplicações se dirijam à mesma para o intercâmbio de dados.

PORTA DE HARDWARE

Soquete numa componente de hardware de um computador, no qual pode ser ligado um cabo ou um conector (porta LPT, porta de série, porta USB).

PORTA DE REDE

Parâmetro TCP e UDP que determina o destino dos pacotes de dados no formato IP, que são transmitidos para um anfitrião através de uma rede, e permite que vários programas em execução num único anfitrião recebam dados independentemente um dos outros. Cada programa processa os dados recebidos através de uma determinada porta (por vezes, para designar isso diz-se que o programa "está a escutar" aquela porta).

Para alguns protocolos de rede comuns, existem normalmente números de porta típicos (por exemplo, os servidores de Internet normalmente recebem pedidos de HTTP na porta 80 do protocolo TCP). Contudo, normalmente, um programa pode utilizar qualquer protocolo em qualquer porta. Valores possíveis: 1 a 65535.

PROCESSO CONFIÁVEL

Processo de aplicações, cujas operações com ficheiros não são monitorizadas pela aplicação da Kaspersky Lab no modo de protecção em tempo real. Por outras palavras, não serão verificados quaisquer objectos executados, abertos ou guardados pelo processo confiável.

PROTECÇÃO EM TEMPO REAL

O modo de funcionamento da aplicação segundo o qual os objectos são verificados, em tempo real, quanto à presença de código malicioso.

A aplicação intercepta todas as tentativas para abrir qualquer objecto (ler, escrever ou executar) e verifica o objecto quanto à presença de ameaças. Os objectos não infectados são disponibilizados ao utilizador, os objectos que contêm ameaças ou que se suspeita conterem ameaças são processados de acordo com as configurações da tarefa (são desinfectados, apagados ou colocados na quarentena).

PROTOCOLO

Conjunto de regras claramente definidas e padronizadas que regulam a interacção entre um cliente e um servidor. Os protocolos mais conhecidos e os serviços a eles associados incluem: HTTP (WWW), FTP e NNTP (notícias).

PROTOCOLO DE INTERNET (IP)

O protocolo de base para a Internet, utilizado sem alterações desde o seu desenvolvimento em 1974. Este executa operações básicas na transmissão de dados de um computador para outro e serve de base para protocolos de nível mais elevado, tais como TCP e UDP. Gere a ligação e o processamento de erros. As tecnologias como a NAT (Conversão de Endereços de Rede) e a utilização de máscaras permitem ocultar um elevado número de redes privadas, utilizando um número reduzido de endereços IP (ou até mesmo um único endereço), o que permite responder às exigências de uma Internet em constante crescimento, utilizando o espaço relativamente restrito de endereços IPv4.

PROTOCOLO SOCKS

Protocolo do servidor de proxy que permite estabelecer uma ligação ponto-a-ponto entre computadores nas redes interna e externa.

QUARENTENA

Uma determinada pasta na qual são colocados todos os objectos possivelmente infectados detectados durante as verificações ou detectados pela protecção em tempo real.

RESTAURO

Mover um objecto original da Quarentena ou da Cópia de Segurança para a pasta onde se encontrava originalmente (antes de ter sido movido para a Quarentena, desinfectado ou apagado) ou para uma pasta diferente especificada pelo utilizador.

SCRIPT

Um pequeno programa de computador ou uma parte independente de um programa (função) que, por norma, é desenvolvida para executar uma pequena tarefa específica. Na maioria dos casos, é utilizado com programas incorporados em hipertexto. Os scripts são executados, por exemplo, quando abre um determinado site.

Se a protecção em tempo real estiver activada, a aplicação irá vigiar a inicialização dos scripts, interceptá-los e verificá-los quanto à presença de vírus. Dependendo do resultado da verificação, você pode bloquear ou permitir a execução de um script.

SECTOR DE INICIALIZAÇÃO DO DISCO

Um sector de inicialização é uma área especial no disco rígido de um computador, numa disquete ou num outro dispositivo de armazenamento de dados. Este sector contém informação sobre o sistema de ficheiros do disco e um programa de carregamento da inicialização, que é responsável por iniciar o sistema operativo.

Existem vários vírus que infectam os sectores de inicialização do disco, por isso são denominados de vírus de inicialização. A aplicação da Kaspersky Lab permite verificar os sectores de inicialização quanto à presença de vírus e desinfectá-los, caso seja detectada uma infecção.

SERVIÇO DE NOMES DE DOMÍNIO (DNS)

Sistema distribuído para converter o nome de um anfitrião (um computador ou outro dispositivo de rede) num endereço IP. O DNS funciona em redes TCP/IP. Em particular, o DNS também pode armazenar e processar pedidos inversos, determinando o nome de um anfitrião a partir do seu endereço IP (registo PTR). A resolução de nomes DNS é normalmente executada por aplicações de rede, não por utilizadores.

SERVIDOR DE PROXY

Serviço de rede do computador, que permite que os utilizadores façam pedidos indirectos a outros serviços de rede. Primeiro, um utilizador liga-se a um servidor de proxy e solicita um recurso (por exemplo, um ficheiro) localizado noutro servidor. Depois, o servidor de proxy liga-se ao servidor especificado e obtém o recurso a partir do mesmo ou devolve o recurso a partir da sua própria memória temporária (caso o servidor de proxy tenha a sua própria memória temporária) Nalguns casos, o pedido de um utilizador ou a resposta de um servidor pode ser alterada pelo servidor de proxy, por algum motivo.

SERVIDORES DE ACTUALIZAÇÃO DA KASPERSKY LAB

Uma lista dos servidores HTTP e FTP da Kaspersky Lab, a partir dos quais a aplicação transfere as actualizações das bases de dados e dos módulos para o seu computador.

SURTO DE VÍRUS

Uma série de tentativas premeditadas para infectar um computador com um vírus.

TAREFA

As funções executadas pela aplicação da Kaspersky Lab são implementadas enquanto tarefas, tais como: Protecção dos ficheiros em tempo real, Verificação completa do computador, Actualização da base de dados.

TECNOLOGIA ICHECKER

iChecker é uma tecnologia que aumenta a velocidade das verificações antivírus, excluindo os objectos que não foram modificados desde a sua última verificação, desde que os parâmetros de verificação (a base de dados antivírus e as definições) não tenham sido alterados. A informação para cada ficheiro é armazenada numa base de dados especial. Esta tecnologia é utilizada nos modos de protecção em tempo real e de verificação sob pedido.

Por exemplo, você tem um arquivo verificado pela aplicação da Kaspersky Lab e ao qual foi atribuído o estado não infectado. Na próxima vez, a aplicação irá ignorar este arquivo, excepto se tiver sido alterado ou se as definições de verificação tiverem sido alteradas. Se você tiver alterado o conteúdo do arquivo, adicionando-lhe um novo objecto, se tiver alterado as definições de verificação ou se tiver actualizado a base de dados antivírus, o arquivo será novamente verificado.

Limitações da tecnologia iChecker:

esta tecnologia não funciona com ficheiros extensos, uma vez que é mais rápido analisar um ficheiro do que verificar se este foi modificado desde a última verificação;

a tecnologia suporta um número limitado de formatos (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

VERIFICAÇÃO DO TRÁFEGO

Uma verificação em tempo real, utilizando a informação da última versão das bases de dados, para os objectos transmitidos através de todos os protocolos (por exemplo, HTTP, FTP, etc.).

VÍRUS DE INICIALIZAÇÃO

Um vírus que infecta os sectores de inicialização do disco rígido de um computador. O vírus obriga o sistema a carregar o vírus na memória durante a reinicialização e a direccionar o controlo para o código do vírus, em vez de para o código original de carregamento da inicialização.

VÍRUS DESCONHECIDO

Um novo vírus sobre o qual não existe informação nas bases de dados. Normalmente, os vírus desconhecidos são detectados pela aplicação nos objectos através do analisador heurístico e esses objectos são classificados como potencialmente infectados.

KASPERSKY LAB

A Kaspersky Lab foi fundada em 1997 e actualmente é a empresa russa líder no desenvolvimento de uma vasta gama de produtos de software de segurança de informação, incluindo sistemas antivírus, anti-spam e anti-hackers.

A Kaspersky Lab é uma empresa internacional. Sediada na Federação Russa, a empresa tem filiais representantes no Reino Unido, França, Alemanha, Japão, Benelux, China, Polónia, Roménia e EUA (Califórnia). Um novo departamento da empresa, o Centro Europeu de Pesquisa Antivírus, foi recentemente criado em França. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas em todo o mundo.

Hoje, a Kaspersky Lab emprega mais de 1000 especialistas altamente qualificados, dos quais 10 têm graduações M.B.A. e 16 têm doutoramentos. Vários especialistas antivírus seniores da Kaspersky Lab são membros da Computer Anti-virus Researchers Organization (CARO).

Os bens mais valiosos da nossa empresa são a experiência e o conhecimento únicos acumulados pelos nossos especialistas ao longo de 14 anos a combater vírus de computador. Uma análise detalhada das actividades dos vírus de computador permite que os especialistas da empresa consigam prever as tendências no desenvolvimento de software malicioso e forneçam aos nossos utilizadores uma protecção atempada contra novos tipos de ataques. Esta vantagem é a base dos produtos e serviços da Kaspersky Lab. Em qualquer altura, os produtos da empresa permanecem um passo à frente dos outros fornecedores no fornecimento de uma cobertura antivírus abrangente para os nossos clientes.

Anos de árduo trabalho tornaram a empresa num dos melhores fabricantes de software antivírus. A Kaspersky Lab foi a primeira empresa a desenvolver muitos dos padrões modernos de software antivírus. O produto emblemático da empresa, o Kaspersky Anti-Virus®, protege com fiabilidade todos os tipos de sistemas de computadores contra ataques de vírus, incluindo estações de trabalho, servidores de ficheiros, sistemas de correio electrónico, firewalls, gateways de Internet e computadores portáteis. As suas ferramentas de gestão fáceis de utilizar maximizam o nível de automação da protecção antivírus para computadores e redes empresariais. Um grande número fabricantes a nível mundial usam o núcleo do Kaspersky Anti-Virus nos seus produtos, incluindo a Nokia ICG (EUA), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab beneficiam de uma ampla gama de serviços adicionais que asseguram tanto o funcionamento estável dos produtos da empresa, assim como a total conformidade com as necessidades específicas dos clientes. Concebemos, implementamos e damos apoio a sistemas empresariais antivírus. A base de dados antivírus da Kaspersky Lab é actualizada a cada hora. A empresa fornece aos seus clientes um serviço de suporte técnico de 24 horas, disponível em várias línguas.

Se tiver alguma questão, comentário ou sugestão, pode contactar-nos através dos nossos distribuidores ou contactar, directamente, a Kaspersky Lab. Teremos todo o prazer em ajudá-lo por telefone ou por e-mail em qualquer assunto relacionado com nossos produtos. Receberá respostas completas e abrangentes a todas as suas questões.

Site oficial da Kaspersky Lab:	http://www.kaspersky.pt
Enciclopédia de Vírus:	http://www.viruslist.com
Laboratório Antivírus:	newvirus@kaspersky.com (apenas para enviar objectos suspeitos em arquivos) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en (para enviar pedidos aos analistas de vírus)
Fórum na Internet da Kaspersky Lab:	http://forum.kaspersky.com

CONTRATO DE LICENÇA

AVISO LEGAL IMPORTANTE A TODOS OS UTILIZADORES: LEIA COM ATENÇÃO O SEGUINTE ACORDO LEGAL ANTES DE COMEÇAR A UTILIZAR O SOFTWARE.

AO CLICAR NO BOTÃO "ACEITAR" NA JANELA DO CONTRATO DE LICENÇA OU AO INTRODUZIR SÍMBOLO(S) CORRESPONDENTE(S) CONCORDA EM ESTAR VINCULADO PELOS TERMOS E CONDIÇÕES DESTE CONTRATO. **ESSA ACÇÃO SIMBOLIZA A SUA ASSINATURA E ESTÁ A CONCORDAR ESTAR VINCULADO AO CONTRATO, CONSTITUINDO UMA PARTE DO MESMO, E CONCORDA QUE ESTE CONTRATO É EXECUTÓRIO COMO QUALQUER OUTRO CONTRATO NEGOCIADO POR ESCRITO E ASSINADO POR SI.** SE NÃO CONCORDAR COM TODOS OS TERMOS E CONDIÇÕES DESTE CONTRATO, CANCELE A INSTALAÇÃO DO SOFTWARE E NÃO O INSTALE.

DEPOIS DE CLICAR NO BOTÃO "ACEITAR" NA JANELA DO CONTRATO DE LICENÇA OU APÓS TER INTRODUZIDO O(S) SÍMBOLO(S) CORRESPONDENTE(S), TEM O DIREITO DE UTILIZAR O SOFTWARE DE ACORDO COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. Definições

1.1. **Software** refere-se ao software, incluindo quaisquer Actualizações e materiais relacionados.

1.2. **Detentor dos Direitos** (proprietário de todos os direitos, quer exclusivos ou relativos ao Software) refere-se à Kaspersky Lab ZAO, uma empresa incorporada de acordo com as leis da Federação Russa.

1.3. **Computador(es)** refere-se ao(s) hardware(s), incluindo os computadores pessoais, portáteis, estações de trabalho, assistentes digitais pessoais, 'smart phones', dispositivos manuais ou outros dispositivos electrónicos para os quais o Software foi concebido e onde o Software será instalado e/ou usado.

1.4. **Utilizador Final** refere-se ao(s) indivíduo(s) que instalam ou utilizam o Software a seu favor ou que utilizam legalmente uma cópia do Software; ou, se o Software for transferido ou instalado em nome de uma organização, quando se refere a um funcionário, *"Utilizador Final"* refere-se ainda à organização para a qual o Software foi transferido ou instalado ficando por este meio claramente definido que essa organização autorizou a pessoa que aceitou este contrato a fazê-lo em seu nome. Para fins deste contrato, o termo *"organização",* sem limitações, inclui quaisquer parcerias, empresas de responsabilidade limitada, corporações, associações, empresas de capitais mistos, empresas de crédito, "joint ventures", sindicatos de trabalho, empresas não constituídas em sociedade ou autoridades governamentais.

1.5. **Parceiro(s)** refere-se a organizações ou indivíduo(s), que distribuem o Software com base num contrato e numa licença do Detentor dos Direitos.

1.6. **Actualização(ões)** refere-se a todas as actualizações, revisões, correcções ("patches"), melhorias, "fixes", modificações, cópias, adições ou pacotes de manutenção, etc.

1.7. **Manual do Utilizador** refere-se ao manual do utilizador, guia do administrador, livro de referências e material explicativo ou de outro tipo relacionado.

2. Concessão de licença

2.1. O Detentor de Direitos concede, por este meio, uma licença de não exclusividade ao Utilizador Final que lhe permite armazenar, carregar, instalar, executar e visualizar (para "utilizar") o Software num número específico de Computadores, tendo como finalidade ajudar a proteger o Computador do Utilizador Final no qual o Software está instalado, contra as ameaças descritas no Manual do Utilizador, de acordo com todos os requisitos técnicos descritos no Manual do Utilizador e com os termos e condições deste Contrato (a "Licença") e o utilizador final aceita esta Licença:

Versão experimental. Se recebeu, transferiu e/ou instalou uma versão experimental do Software sendo-lhe por este meio concedida uma licença de avaliação para o Software, só pode utilizar o Software para fins de avaliação e apenas durante o período de avaliação único aplicável, a não ser se indicado o contrário, a contar da data da instalação inicial. A utilização do Software para outros fins ou para além do período de avaliação aplicável é estritamente proibida.

Software de vários ambientes; Software de vários idiomas; Software de dualidade de multimédia; várias cópias; pacotes. Se utilizar versões diferentes do Software ou edições do Software em idiomas diferentes, se receber o Software em vários suportes, se receber várias cópias do Software ou se receber o Software num pacote junto com outro software, o número total permitido de Computadores em que as versões do Software estão instaladas devem corresponder ao número total de licenças obtidas junto do Detentor dos Direitos e, *a não ser* que os termos da licença indiquem o contrário, cada licença adquirida dá-lhe o direito de instalar e utilizar o Software nessa quantidade de Computador(es), como especificado nas Cláusulas 2.2 e 2.3.

2.2. Se o Software foi adquirido num meio físico, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na embalagem do Software.

2.3. Se o Software foi adquirido através da Internet, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na Licença do Software quando adquirido.

2.4. Tem o direito de fazer uma cópia do Software apenas para fins de cópia de segurança e apenas para substituir a cópia legal caso essa cópia se perca, seja destruída ou fique inutilizada. Esta cópia de segurança não pode ser utilizada para outros fins e tem de ser destruída se perder o direito de utilização do Software ou quando a licença de Utilizador Final expirar ou for rescindida por qualquer outra razão, de acordo com a legislação em vigor no país de residência principal do Utilizador Final ou no país onde o mesmo está a utilizar o Software.

2.5. Pode transferir a licença de não exclusividade de utilização do Software a outras pessoas ou entidades legais, no âmbito da licença que o Detentor dos Direitos concedeu ao Utilizador Final, desde que o destinatário concorde em ficar vinculado por todos os termos e condições deste Contrato e que substitua na totalidade o primeiro Utilizador Final no que se refere à licença concedida por parte do Detentor dos Direitos. Caso o Utilizador Final transfira todos os direitos concedidos pelo Detentor dos Direitos para utilização do Software, o Utilizador Final tem de destruir todas as cópias do Software, incluindo a cópia de segurança. Se o Utilizador Final é já um destinatário de uma licença transferida, tem de concordar com o cumprimento de todos os termos e condições deste Contrato. Se não concorda com todos os termos e condições deste Contrato, o Utilizador Final não pode instalar e/ou utilizar o Software. Na qualidade de destinatário de uma licença transferida, concorda ainda que não tem direitos adicionais nem melhores do que o Utilizador Final original que adquiriu o Software ao Detentor dos Direitos.

2.6. A partir do momento em que o Software foi activado ou que o ficheiro da chave de licença foi instalado (à excepção de uma versão experimental do Software), tem o direito de receber os seguintes serviços pelo período definido especificado na embalagem de Software (se o Software foi adquirido num meio físico) ou especificado durante a compra (se o Software foi adquirido através da Internet):

- Actualizações do Software através da Internet quando e como o Detentor dos Direitos os publicar no seu próprio website ou através de outros serviços online. Quaisquer Actualizações que possa receber passam a fazer parte do Software e os termos e condições deste Contrato aplicam-se às mesmas;
- Assistência técnica através da Internet e assistência técnica através de uma linha telefónica grátis.

3. Activação e Termo

3.1. Se o Utilizador Final modificar o seu Computador ou fizer alterações ao software de outros fabricantes instalado nesse mesmo Computador, o Detentor dos Direitos poderá exigir que repita a activação do Software ou a instalação do ficheiro da chave de licença. O Detentor dos Direitos reserva-se o direito de utilizar quaisquer meios ou procedimentos de verificação para confirmar a validade da Licença e/ou a legalidade de uma cópia instalada do Software e/ou utilizada no Computador do Utilizador Final.

3.2. Se o Software foi adquirido num meio físico, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado na embalagem. Esse período terá início a partir do momento de aceitação deste Contrato.

3.3. Se o Software foi adquirido através da Internet, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado durante a compra.

3.4. Tem o direito de utilizar uma versão experimental do Software, como disposto na Cláusula 2.1 sem que tenha de pagar nada durante o período de avaliação (30 dias) desde o momento em que o Software é activado, de acordo com este Contrato, *desde que* a versão experimental não de ao Utilizador Final acesso a Actualizações e a assistência técnica através da Internet e da linha telefónica.

3.5. A Licença para Utilização do Software está limitada ao período de tempo especificado nas Cláusulas 3.2 ou 3.3 (como aplicável) e o restante período pode ser visto através dos meios descritos no Manual do Utilizador.

3.6. Se tiver adquirido o Software que se destina a ser usado em mais do que um Computador, a sua Licença para Usar o Software estará limitada ao período de tempo que tem início com a data de activação do Software ou da instalação do ficheiro da chave de licença no primeiro Computador.

3.7. Sem prejuízo de quaisquer recursos legais ou de justiça natural que o Detentor dos Direitos possa ter, caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final, o Detentor dos Direitos pode, em qualquer altura e sem qualquer aviso prévio ao Utilizador Final, rescindir esta Licença de utilização do Software sem reembolsar o preço de compra ou qualquer outra parte do mesmo.

3.8. Concorda que, ao utilizar o Software e qualquer relatório ou informações derivadas resultantes da utilização deste Software, irá cumprir todas as leis e regulamentos internacionais, nacionais, estatais, regionais e locais aplicáveis, incluindo, mas não se limitando às leis da privacidade, direitos de autor, controlo de exportação e obscenidade.

3.9. Excepto quando especificamente indicado neste documento, não pode transferir nem atribuir a terceiros nenhum dos direitos a si concedidos, ao abrigo deste Contrato, nem nenhuma das suas obrigações em conformidade com o presente.

4. Assistência técnica

A assistência técnica descrita na Cláusula 2.6 deste Contrato é fornecida ao Utilizador Final depois de ter sido instalada a mais recente Actualização do Software (excepto quando se trata de uma versão experimental do Software).
Serviço de assistência técnica: http://support.kaspersky.com.

5. Recolha de informações

5.1. Depois de concordar com os termos e condições deste Contrato, o Utilizador Final consente em fornecer informações ao Detentor dos Direitos sobre os ficheiros executáveis e as suas somas de verificação para melhorar o seu próprio nível de protecção de segurança.

5.2. Para melhorar a consciência de segurança sobre novas ameaças e as suas origens, e para melhorar o nível de segurança da protecção do Utilizador Final, o Detentor dos Direitos, com o consentimento do Utilizador Final, explicitamente confirmado na Kaspersky Security Network Data Collection Statement (Declaração de Recolha de Dados da Rede de Segurança da Kaspersky), tem o direito expresso de receber estas informações. Pode desactivar o serviço Kaspersky Security Network (Rede de segurança da Kaspersky) durante a instalação. Além disso, pode activar e desactivar o serviço Kaspersky Security Network (Rede de segurança da Kaspersky) em qualquer altura na página de opções do Software.

Aceita e concorda ainda que, todas as informações reunidas pelo Detentor dos Direitos podem ser utilizadas para seguir e publicar relatórios sobre as tendências dos riscos de segurança, de acordo com os critérios próprios e exclusivos do Detentor dos Direitos.

5.3. O Software não processa quaisquer dados pessoalmente identificáveis e não combina os dados de processamento com quaisquer informações pessoais.

5.4. Se não pretende que as informações recolhidas pelo Software sejam enviadas para o Detentor dos Direitos, o Utilizador Final não deve activar e/ou desactivar o serviço Kaspersky Security Network (Rede de segurança da Kaspersky).

6. Limitações

6.1. Não deve emular, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar ou inverter a engenharia do Software, nem desmontar ou criar trabalhos dele derivados e baseados no Software ou em qualquer parte do mesmo, sendo que a única excepção é a existência de um direito sem limitações concedido ao Utilizador Final pela legislação aplicável, bem como não pode reduzir qualquer parte do Software a uma forma legível, nem transferir o Software licenciado, ou qualquer outro subconjunto do Software licenciado, nem permitir que terceiros o façam, excepto até ao ponto em que as restrições indicadas sejam expressamente proibidas pela lei aplicável. Não se pode utilizar o código de binários nem a fonte do Software, nem inverter a engenharia, para recriar o algoritmo do programa, que é registado. Todos os direitos que não são aqui expressamente concedidos são reservados pelo Detentor dos Direitos e/ou pelos seus fornecedores, como aplicável. Qualquer utilização não autorizada do Software resultará na rescisão imediata e automática deste Contrato e da Licença concedida pelo mesmo e pode resultar em processos criminais e/ou civis contra o Utilizador Final.

6.2. Não pode transferir os direitos de utilização do Software para terceiros, excepto conforme disposto na Cláusula 2.5 deste Contrato.

6.3. Não pode fornecer o código de activação e/ou a ficheiro com a chave da licença a terceiros nem permitir que terceiros acedam ao código de activação e/ou chave da licença que são considerados dados confidenciais do Detentor dos Direitos e terá todo o cuidado em proteger o código de activação e/ou chave da licença contando que pode transferir o código de activação e/ou a chave de licença a terceiros como definido na cláusula 2.4 deste Contrato.

6.4. Não pode alugar, arrendar ou emprestar o Software a terceiros.

6.5. Não pode utilizar o Software para criação de dados ou de software utilizado para a detecção, bloqueio ou tratamento das ameaças descritas no Manual do Utilizador.

6.6. O Detentor dos Direitos tem o direito de bloquear o ficheiro da chave ou rescindir a Licença de utilização do Software caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final sem qualquer reembolso.

6.7. Se o Utilizador Final está a utilizar a versão experimental do Software, não tem o direito de receber a Assistência Técnica especificada na Cláusula 4 deste Contrato e o Utilizador Final não tem o direito de transferir a licença ou os direitos de utilização do Software a terceiros.

7. Garantia limitada e Renúncias

7.1. O Detentor dos Direitos garante que o Software irá cumprir substancialmente o que lhe é devido, de acordo com as especificações e descrições indicadas no Manual do Utilizador *desde que, no entanto,* essa garantia limitada não se aplique ao seguinte: (w) As deficiências e violações relacionadas do computador para as quais o Detentor dos Direitos renuncia expressamente todas as responsabilidades da garantia; (x) avarias, defeitos ou falhas resultantes de má utilização; abuso; acidente; negligência; instalação imprópria, operação ou manutenção; roubo; vandalismo; casos fortuitos; actos de terrorismo; falhas de energia ou picos de potência; acidentes; alterações, modificações não permitidas ou reparações por qualquer parte além do Detentor de Direitos; ou as acções do Utilizador Final ou causas que estejam para além do controlo razoável do Detentor dos Direitos; (y) qualquer defeito que o Utilizador Final não tenha dado a conhecer ao Detentor de Direitos logo que possível depois de o defeito aparecer pela primeira vez; e (z) incompatibilidade provocada pelos componentes de hardware e/ou software instalados no Computador do Utilizador Final.

7.2. O Utilizador Final reconhece, aceita e concorda que não existe nenhum software isento de erros e o Utilizador Final é aconselhado a fazer cópias de segurança do Computador, com a frequência e a fiabilidade adequada para o Utilizador Final.

7.3. O Detentor dos Direitos não oferece qualquer garantia de que o Software irá funcionar correctamente em caso de violações dos termos descritos no Manual do Utilizador ou neste Contrato.

7.4. O Detentor dos Direitos não garante que o Software irá funcionar correctamente se o Utilizador Final não fizer regularmente transferências das Actualizações especificadas na Cláusula 2.6 deste Contrato.

7.5. O Detentor dos Direitos não garante protecção das ameaças descritas no Manual do Utilizador após a expiração do período especificado nas Cláusulas 3.2 ou 3.3 deste Contrato ou após a rescisão da Licença de utilização do Software, caso ela seja rescindida por qualquer razão.

7.6. O SOFTWARE É ENTREGUE "TAL COMO ESTÁ" E O DETENTOR DOS DIREITOS NÃO FAZ QUALQUER REPRESENTAÇÃO NEM DÁ QUAISQUER GARANTIAS DA SUA UTILIZAÇÃO OU DESEMPENHO. EXCEPTO NO QUE SE REFERE A QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO NA MEDIDA EM QUE NÃO POSSA SER EXCLUÍDA OU LIMITADA PELA LEI APLICÁVEL, O DETENTOR DOS DIREITOS E OS SEUS PARCEIROS NÃO CONCEDEM QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO (EXPRESSO OU IMPLÍCITO, QUER SEJA POR ESTATUTO, LEI COMUM, PERSONALIZAÇÃO, UTILIZAÇÃO OU QUALQUER OUTRO) QUE, SEM OUTRO ASSUNTO INCLUINDO, MAS NÃO SE LIMITANDO, A NÃO INFRACÇÃO DOS DIREITOS DE TERCEIROS, COMERCIALIZAÇÃO, QUALIDADE SATISFATÓRIA, INTEGRAÇÃO OU APLICABILIDADE A UM FIM ESPECÍFICO. O UTILIZADOR FINAL ASSUME TODAS AS AVARIAS E TODO O RISCO DE DESEMPENHO E RESPONSABILIDADE POR SELECCIONAR O SOFTWARE DE MODO A CONSEGUIR OS RESULTADOS PRETENDIDOS, E PELA INSTALAÇÃO, UTILIZAÇÃO E RESULTADOS OBTIDOS DO SOFTWARE. SEM LIMITAR AS DISPOSIÇÕES ANTERIORES, O DETENTOR DOS DIREITOS NÃO CONCEDE QUALQUER REPRESENTAÇÃO E NÃO DÁ GARANTIAS DE QUE O SOFTWARE NÃO CONTÉM ERROS OU NÃO ESTÁ LIVRE DE INTERRUPÇÕES OU OUTRAS FALHAS OU QUE O SOFTWARE VAI AO ENCONTRO DE TODOS E QUAISQUER REQUISITOS DO UTILIZADOR FINAL TENHAM OU NÃO SIDO DIVULGADOS AO DETENTOR DOS DIREITOS.

8. Exclusão e limitação da responsabilidade

NA MEDIDA MÁXIMA PERMITIDA PELA LEI APLICÁVEL, EM CASO ALGUM O DETENTOR DOS DIREITOS OU OS SEUS PARCEIROS SÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, ACIDENTAIS, PUNITIVOS, INDIRECTOS OU CONSEQUENCIAIS, SEJAM ELES QUAIS FOREM, (INCLUINDO, MAS NÃO SE LIMITANDO A DANOS POR PERDA DE LUCROS OU DE INFORMAÇÕES CONFIDENCIAIS, OU OUTRAS, POR INTERRUPÇÃO DO NEGÓCIO, POR PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANOS E PERDAS DE DADOS OU PROGRAMAS, POR FALHA DE PAGAMENTO DE QUAISQUER DIREITOS INCLUINDO QUAISQUER DIREITOS LEGAIS, DIREITOS DE LEALDADE OU DIREITOS DE CUIDADOS RAZOÁVEIS, POR NEGLIGÊNCIA, POR PERDA ECONÓMICA, E POR QUALQUER PERDA PECUNIÁRIA OU OUTRA, SEJA ELA QUAL FOR) QUE SURJA DE UMA QUALQUER FORMA RELACIONADA COM A UTILIZAÇÃO OU INCAPACIDADE DE UTILIZAÇÃO DO SOFTWARE, A DISPOSIÇÃO OU FALHA DE FORNECIMENTO DE ASSISTÊNCIA OU OUTROS SERVIÇOS, INFORMAÇÕES, SOFTWARE E CONTEÚDOS RELACIONADOS ATRAVÉS DO SOFTWARE OU QUE, POR OUTRO LADO, SURJA DA UTILIZAÇÃO DO SOFTWARE, OU, AO CONTRÁRIO, MEDIANTE OU EM LIGAÇÃO A QUALQUER DISPOSIÇÃO DESTE CONTRATO, OU QUE SURJA DE QUALQUER VIOLAÇÃO DO CONTRATO OU QUALQUER DELITO (INCLUINDO NEGLIGÊNCIA, MÁ REPRESENTAÇÃO OU QUALQUER OBRIGAÇÃO OU DEVER DE RESPONSABILIDADE LIMITADA), OU QUALQUER VIOLAÇÃO DOS DEVERES LEGAIS, OU QUALQUER VIOLAÇÃO DA GARANTIA DO DETENTOR DOS DIREITOS OU QUALQUER UM DOS SEUS PARCEIROS, MESMO QUE O DETENTOR DOS DIREITOS OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DESSES DANOS.

O UTILIZADOR FINAL CONCORDA QUE, CASO O DETENTOR DOS DIREITOS E/OU OS SEUS PARCEIROS SEJAM TIDOS COMO RESPONSÁVEIS, A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS DEVE SER LIMITADA PELOS CUSTOS DO SOFTWARE. EM CASO ALGUM DEVE A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS EXCEDER AS TAXAS PAGAS PELO SOFTWARE AO DETENTOR DOS DIREITOS OU AO PARCEIRO (COMO SE APLICAR).

NADA NESTE ACORDO EXCLUI OU LIMITA QUAISQUER REIVINDICAÇÕES DE MORTE E FERIMENTOS PESSOAIS. ALÉM DISSO, NO CASO DE ALGUMA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NESTE CONTRATO NÃO POSSAM SER EXCLUÍDAS OU LIMITADAS DE ACORDO COM A LEI APLICÁVEL, ENTÃO APENAS ESSA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NÃO SE DEVEM APLICAR AO UTILIZADOR FINAL E CONTINUA A FICAR VINCULADO POR TODAS AS RESTANTES RESPONSABILIDADES, EXCLUSÕES E LIMITAÇÃO.

9. GNU e outras licenças de terceiros

O Software pode incluir alguns programas de software licenciados (ou sublicenciados) ao utilizador no âmbito da Licença Pública Geral GNU (General Public License, GPL) ou outras licenças semelhantes de software grátis que, entre outros direitos, permite ao utilizador copiar, modificar e redistribuir determinados programas, ou partes do mesmo, e ter acesso ao código fonte ("Software de Código Aberto"). Se essas licenças necessitarem que, para qualquer software que é distribuído às pessoas num formato de binário executável, que o código fonte também seja tornado disponível a esses utilizadores, então o código fonte deve ser tornado disponível enviando o pedido para source@kaspersky.com ou é fornecido com o Software. Se quaisquer licenças de Software de Código Aberto precisarem que o Detentor dos Direitos forneça direitos de utilização, cópia ou modificação de um programa de Software de Código Aberto, mais vastos do que os direitos concedidos neste Contrato, então esses direitos devem ter precedência sobre os direitos e restrições aqui indicados.

10. Posse dos direitos de propriedade

10.1 Concorda que o Software e a respectiva autoria, os sistemas, ideias, métodos de funcionamento, documentação e outras informações contidas no Software, são propriedade intelectual registada e/ou segredo comercial, de grande valor, do Detentor dos Direitos ou dos seus parceiros e que o Detentor dos Direitos e os seus parceiros, conforme aplicável, estão protegidos pela lei civil e criminal e pelas leis de direitos de autor, segredos comerciais, marcas registadas e patentes da Federação Russa, União Europeia e Estados Unidos e de outros países, bem como pelos tratados internacionais. Este Contrato não concede ao Utilizador Final quaisquer direitos no que se refere à propriedade intelectual, incluindo as marcas comerciais ou as marcas dos serviços do Detentor dos Direitos e/ou dos seus parceiros ("Marcas Comerciais"). Pode utilizar as Marcas Comerciais apenas e até ao ponto de identificar resultados impressos produzidos pelo Software de acordo com a prática das marcas comerciais aceites, incluindo a identificação do nome do proprietário da Marca Comercial. A utilização de qualquer Marca Comercial não dá ao Utilizador Final quaisquer direitos de propriedade sobre essa Marca Comercial. O Detentor dos Direitos e/ou os seus parceiros são proprietários e retêm todos os direitos, títulos e interesse no Software e em relação ao mesmo, incluindo, sem limitações, quaisquer correcções de erros, melhoramentos, Actualizações ou outras modificações ao Software, quer sejam feitas pelo Detentor dos Direitos ou por quaisquer terceiros, e todos os direitos sobre direitos de autor, patentes, segredos comerciais, marcas comerciais e outras propriedades intelectuais contidas neste documento. A possessão, instalação ou utilização do Software não lhe transfere qualquer título para a propriedade intelectual no Software e não adquire quaisquer direitos ao Software excepto quando expressamente estipulado neste Contrato. Todas as cópias do Software realizadas nos termos do presente Contrato têm de conter os mesmos avisos de propriedade que aparecem no Software. Excepto como aqui indicado, este Contrato não concede ao Utilizador Final quaisquer direitos de propriedade intelectual sobre o Software e o Utilizador Final reconhece que a Licença, tal como está definida aqui, concedida nos termos deste Contrato, concede apenas o direito de utilização limitada mediante os termos e as condições deste Contrato. O Detentor dos Direitos reserva-se todos os direitos não expressamente concedidos ao Utilizador Final neste Contrato.

10.2 O Utilizador Final reconhece que o código fonte, o código de activação e/ou o ficheiro da chave da licença do Software são propriedade do Detentor dos Direitos e constituem segredos comerciais do Detentor dos Direitos. Concorda em não modificar, adaptar, traduzir, inverter a engenharia, descompilar, desmontar ou tentar, de qualquer outro modo, descobrir o código fonte do Software seja de que forma for.

10.3 Concorda em não modificar nem alterar o Software seja de que forma for. Não pode remover nem alterar quaisquer avisos de direitos de autor ou outros avisos de propriedade em nenhuma cópia do Software.

11. Lei vigente; arbitragem

Este Contrato é regido, e será interpretado, de acordo com as leis da Federação Russa sem referência a conflitos de regras e princípios legais. Este Contrato não será regido pela Convenção das Nações Unidas referente a Contratos para a Venda Internacional de Bens, a aplicação da qual é expressamente excluída. Qualquer litígio que surja no seguimento da interpretação ou aplicação dos termos deste Contrato ou qualquer infracção ao mesmo, a não ser que se resolva por negociação directa, deverá ser resolvido no Tribunal de Arbitragem Comercial Internacional na Câmara do Comércio e Indústria da Federação Russa em Moscovo, na Federação Russa. Qualquer decisão apresentada pelo árbitro deve ser final e obrigatória para as partes e qualquer julgamento sobre essa decisão de arbitragem pode ser feita cumprir em qualquer tribunal da jurisdição competente. Nada nesta Secção 11 deve impedir que uma Parte procure e obtenha qualquer reparação equitativa de um tribunal da jurisdição competente, quer seja antes, durante ou depois dos processos de arbitragem.

12. Período para interpor acções.

Nenhuma acção, independentemente da forma, que surja das transacções nos termos deste Contrato, pode ser trazida aqui por qualquer uma das partes mais de um (1) ano depois da causa da acção ter ocorrido, ou de ter sido descoberta a ocorrência, excepto que uma acção por violação dos direitos de propriedade intelectual seja trazida dentro do período legal máximo aplicável.

13. Contrato completo; redução; sem renúncia.

Este Contrato constitui todo o contrato entre o Utilizador Final e o Detentor dos Direitos e substitui quaisquer outros acordos prévios, propostas, comunicações ou publicidade, oral ou escrita, referente ao Software ou ao assunto deste Contrato. O Utilizador Final reconhece que leu este Contrato, compreendeu-o e concorda em estar vinculado pelos seus termos. Se qualquer disposição deste Contrato for indicada por um tribunal de jurisdição competente como sendo inválida, nula ou inexequível por qualquer razão, no todo ou em parte, essa disposição será ainda mais restritamente interpretada de tal forma que será legal e executória, e todo o Contrato não falhará por conta do mesmo e o saldo do Contrato continuará válido e com efeitos até ao máximo permitido por lei ou equidade ao mesmo tempo que preserva, até ao máximo possível, a sua intenção original. Nenhuma renúncia de nenhuma disposição ou condição aqui indicadas será válida a não ser por escrito e assinada pelo Utilizador Final e um representante autorizado do Detentor dos Direitos desde que nenhuma renúncia de nenhuma infracção de nenhuma disposição deste Contrato constitua uma renúncia de qualquer infracção anterior, concorrente ou subsequente. A não insistência por parte do Detentor dos Direitos no que se refere a fazer valer o desempenho rigoroso de todas as disposições deste Contrato ou nenhum direito deve ser interpretado como sendo uma renúncia de qualquer uma dessas disposições ou direitos.

14. Informações de contacto.

Se tiver quaisquer dúvidas referentes a este Contrato ou se, por qualquer razão, pretender contactar o Detentor dos Direitos, contacte o nosso Departamento de Apoio ao Cliente em:

Kaspersky Lab ZAO, 10 build. 1 1st Volokolamsky Proezd
Moscovo, 123060
Federação Russa
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Website: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. Todos os direitos reservados. O Software e toda a documentação que o acompanha têm direitos de autor e estão protegidos pelas leis de direitos de autor e por tratados internacionais de direitos de autor, bem como por outras leis e tratados de propriedade intelectual.

ÍNDICE

A

Activar / desactivar a protecção em tempo real 95
Actualização
  a partir de uma pasta local 91
  configurações regionais 90
  origem de actualização 89
  reverter a última actualização 89
  usar um servidor de proxy 90
Agendamento
  actualização 92
  verificação de vírus 81
Algoritmo de funcionamento
  Antivírus de E-mail 53
  Antivírus de Ficheiros 43
  Antivírus de Internet 60
Âmbito de Protecção
  Antivírus de E-mail 55
  Antivírus de Ficheiros 45
  Antivírus de MI 67
Análise heurística
  Antivírus de E-mail 57
  Antivírus de Ficheiros 46
  Antivírus de Internet 64
  Antivírus de MI 68
Antivírus de E-mail
  algoritmo de funcionamento 53
  âmbito de protecção 55
  análise heurística 57
  filtrar anexos 58
  nível de segurança 54
  reacção à ameaça 54
  verificação de ficheiros compostos 57
Antivírus de Ficheiros
  algoritmo de funcionamento 43
  âmbito de protecção 45
  análise heurística 46
  modo de verificação 48
  nível de segurança 44
  optimização da verificação 47
  pausar 49, 50
  restaurar as predefinições 51
  restaurar as predefinições 58
  tecnologia de verificação 49
  verificação de ficheiros compostos 47, 48
Antivírus de Internet
  algoritmo de funcionamento 60
  análise heurística 64
  base de dados de endereços de phishing 62
  nível de segurança 61
  optimização da verificação 64
  reacção à ameaça 61
Antivírus de MI
  âmbito de protecção 67
  análise heurística 68

base de dados de endereços de phishing 68
Armazenamento de cópias de segurança 115
Autodefesa da aplicação 101

B

Base de dados de endereços de phishing
Antivírus de Internet 62
Antivírus de MI 68

C

Categorias de ameaças detectáveis 105
Componentes da aplicação 15
Configuração do navegador 122

D

Defesa Pró-activa
controlo das contas do sistema 71
lista de actividades perigosas 69
regra de monitorização de actividades perigosas 70
Desempenho do Computador 103
Disco de recuperação 120

I

Ícone na área de notificação da da barra de ferramentas 37
INTERFACE DA APLICAÇÃO 37

J

Janela principal da aplicação 39

K

Kaspersky Anti-Virus
iniciar com a inicialização do sistema operativo 95

M

Menu de contexto 38

N

Nível de Segurança
Antivírus de E-mail 54
Antivírus de Ficheiros 44
Antivírus de Internet 61

Q

Quarentena 114
Quarentena e Cópia de segurança 114

R

Reacção à ameaça
Antivírus de E-mail 54
Antivírus de Internet 61
Reacção a uma ameaça
verificação de vírus 76
Rede
ligações encriptadas 109
Relatórios
filtragem 130

guardar num ficheiro ... 129
procura de eventos ... 131
seleccionar uma componente ou uma tarefa ... 126
tipo de eventos ... 127
RELATÓRIOS ... 125
Restaurar as predefinições
Antivírus de E-mail ... 58
Antivírus de Ficheiros ... 51
Restringir o acesso à aplicação ... 96

T

Teclado virtual ... 119

V

Verificação
acção sobre objectos detectados ... 76
agendamento ... 81
conta ... 82
execução automática de uma tarefa ignorada ... 81
iniciar uma tarefa ... 74
nível de segurança ... 76
optimização da verificação ... 78
tecnologias de verificação ... 80
tipo de objectos a verificar ... 77
verificação de ficheiros compostos ... 79
verificação de vulnerabilidades ... 83
Verificação de vulnerabilidades
agendamento ... 85
conta ... 86
lista de objectos a verificar ... 84

Z

Zona confiável
aplicações confiáveis ... 105
regras de exclusão ... 106